19. Wahlperiode

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Wortprotokoll
der 124. Sitzung

Ausschuss für Inneres und Heimat
Berlin, den 1. März 2021, 14:00 Uhr
Berlin
Konrad-Adenauer-Str. 1, 10557
Paul-Löbe-Haus, Raum E 700

Vorsitz: Andrea Lindholz, MdB

Tagesordnung - Öffentliche Anhörung

Tagesordnungspunkt **Seite 7**

a) Gesetzentwurf der Bundesregierung

Entwurf eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme

BT-Drucksache 19/26106

Federführend:
Ausschuss für Inneres und Heimat

Mitberatend:
Ausschuss für Recht und Verbraucherschutz
Verteidigungsausschuss
Ausschuss für Verkehr und digitale Infrastruktur
Ausschuss Digitale Agenda
Haushaltsausschuss (mb und § 96 GO)

Gutachtlich:
Parlamentarischer Beirat für nachhaltige Entwicklung

Berichterstatter/in:
Abg. Christoph Bernstiel [CDU/CSU]
Abg. Sebastian Hartmann [SPD]
Abg. Joana Cotar [AfD]
Abg. Manuel Höferlin [FDP]
Abg. Petra Pau [DIE LINKE.]
Abg. Dr. Konstantin von Notz [BÜNDNIS 90/DIE GRÜNEN]

b) Antrag der Abgeordneten Joana Cotar, Uwe Schulz, Dr. Michael Espendiller, weiterer Abgeordneter und der Fraktion der AfD

Evaluierung des IT-Sicherheitsgesetzes von 2015 nach Gesetzeslage umsetzen und Ergebnisse im IT-Sicherheitsgesetz 2.0 berücksichtigen

BT-Drucksache 19/26225

Federführend:
Ausschuss für Inneres und Heimat

Mitberatend:
Ausschuss für Recht und Verbraucherschutz
Ausschuss Digitale Agenda

Berichterstatter/in:
Abg. Christoph Bernstiel [CDU/CSU]
Abg. Sebastian Hartmann [SPD]
Abg. Joana Cotar [AfD]
Abg. Manuel Höferlin [FDP]
Abg. Petra Pau [DIE LINKE.]
Abg. Dr. Konstantin von Notz [BÜNDNIS 90/DIE GRÜNEN]

c) Antrag der Abgeordneten Uwe Schulz, Joana Cotar, Dr. Michael Espendiller und der Fraktion der AfD

IT-Sicherheitsgesetz 2.0 – Planungs- und Rechtssicherheit für Netzbetreiber herstellen

BT-Drucksache 19/26226

Federführend:
Ausschuss für Inneres und Heimat

Mitberatend:
Ausschuss für Recht und Verbraucherschutz
Ausschuss für Verkehr und digitale Infrastruktur
Ausschuss Digitale Agenda

Berichterstatter/in:
Abg. Christoph Bernstiel [CDU/CSU]
Abg. Sebastian Hartmann [SPD]
Abg. Joana Cotar [AfD]
Abg. Manuel Höferlin [FDP]
Abg. Petra Pau [DIE LINKE.]
Abg. Dr. Konstantin von Notz [BÜNDNIS 90/DIE GRÜNEN]

Inhaltsverzeichnis

	Seite
I. Teilnehmerliste	5
II. Sachverständigenliste	6
III. Wortprotokoll der Öffentlichen Anhörung	7
IV. Anlagen	
Anlage A	
Stellungnahmen der Sachverständigen	
Sebastian Artz, Bitkom e. V., Berlin — 19(4)741 A	38
Dr. Sven Herpig, Stiftung Neue Verantwortung e. V., Berlin — 19(4)741 B	57
Manuel Atug, AG KRITIS, Bonn — 19(4)741 C	70
Martin Schallbruch, Digital Society Institute des ESMT Berlin — 19(4)741 D	92
Prof. Dr. Klaus F. Gärditz, Rheinische Friedrich-Wilhelms-Universität Bonn — 19(4)741 E	108
Linus Neumann, Chaos Computer Club Berlin — 19(4)741 F	119
Anlage B	
Unaufgeforderte Stellungnahmen	
Stiftung Neue Verantwortung - Vorläufige Bewertung vom 7.5.2020 — 19(4)512	163
Stiftung Neue Verantwortung vom 1.12.2020 — 19(4)662 neu	174
AG KRITIS, Bonn — 19(4)664	186
BfDI, Bonn — 19(4)681	201
Fachbereich Sicherheit - Schutz und Zuverlässigkeit, Berlin — 19(4)714	205
AOK-Bundesverband, Berlin — 19(4)721	210
VDV Die Verkehrsunternehmen, Köln/Berlin — 19(4)726	216
UP KRITIS Wirtschaftsbeirat — 19(4)727	218
Bundesverband Paket und Express Logistik, Berlin — 19(4)728	229
Gesamtverband der deutschen Versicherungswirtschaft e. V., Berlin — 19(4)740	232

Bundesärztekammer, Berlin	19(4)743	234
Deutsche Krankenhausgesellschaft e.V., Berlin	19(4)744	238
VATM e. V., Köln	19(4)745	246
eco Verband der Internetwirtschaft e.V., Berlin	19(4)747	258
Telefonica Deutschland, Berlin	19(4)748	263
Deutscher Industrie- und Handelskammertag, Berlin	19(4)749	286
ARD, ZDF und Deutschlandradio	19(4)750	295
Die Familienunternehmer e.V., Berlin	19(4)751	307
BDEW Bundesverband der Energie- und Wasserwirtschaft e. V., Berlin	19(4)753	314
DIN e. V., Berlin und DKE, Frankfurt am Main	19(4)759	337

Teilnehmerliste

	Ordentliche Mitglieder	**Stellvertretende Mitglieder**	**Weitere Teilnehmer**
CDU/CSU	Amthor, Philipp Bernstiel, Christoph Lindholz, Andrea Throm, Alexander, Warken, Nina		Schipanski, Tankred
SPD	Hartmann, Sebastian		Mohrs, Falko
AfD		Cotar, Joana	
FDP	Höferlin, Manuel		
DIE LINKE.	Pau, Petra		
BÜNDNIS 90/ DIE GRÜNEN	Domscheit-Berg, Anke Rößner, Tabea		
fraktionslos			

Liste der Sachverständigen

Öffentliche Anhörung am Montag, 1. März 2021, 14.00 Uhr
„IT-Sicherheit“

Sebastian Artz
Bitkom e. V., Berlin

Manuel Atug
AG KRITIS, Bonn

Prof. Dr. Klaus F. Gärditz
Rheinische Friedrich-Wilhelms-Universität Bonn

Dr. Sven Herpig
Stiftung Neue Verantwortung e. V., Berlin

Linus Neumann
Chaos Computer Club Berlin

Martin Schallbruch
Digital Society Institute des ESMT Berlin

Tagesordnungspunkt

a) Gesetzentwurf der Bundesregierung

Entwurf eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme

BT-Drucksache 19/26106

b) Antrag der Abgeordneten Joana Cotar, Uwe Schulz, Dr. Michael Espendiller, weiterer Abgeordneter und der Fraktion der AfD

Evaluierung des IT-Sicherheitsgesetzes von 2015 nach Gesetzeslage umsetzen und Ergebnisse im IT-Sicherheitsgesetz 2.0 berücksichtigen

BT-Drucksache 19/26225

c) Antrag der Abgeordneten Uwe Schulz, Joana Cotar, Dr. Michael Espendiller und der Fraktion der AfD

IT-Sicherheitsgesetz 2.0 – Planungs- und Rechtssicherheit für Netzbetreiber herstellen

BT-Drucksache 19/26226

Vors. **Andrea Lindholz** (CDU/CSU): Ich freue mich, dass wir uns alle hören können und frage kurz ab, wer alles da ist: Herr Sachverständiger Atug in der Leitung, Herr Professor Gärditz ist da, Herr Dr. Herpig ist da. Vielen Dank. Dann Herr Schallbruch ist auch in der Leitung. Vielen Dank. Hier im Raum sind Herr Neumann als Sachverständiger und Herr Artz. Damit darf ich erst mal alle Sachverständigen ganz herzlich begrüßen neben den Kolleginnen und Kollegen hier im Raum. Es müssten noch zugeschaltet sein – sind sie aber glaube ich noch nicht – Frau Rößner von der Fraktion BÜNDNIS 90/DIE GRÜNEN, Frau Domscheit-Berg, Fraktion DIE LINKE, ist bereits da und die Abgeordnete Nina Warken wollte auch noch zugeschaltet sein. Vielleicht kommen die beiden noch. Auch den Kolleginnen und Kollegen erst mal ein herzliches Grüß Gott heute. Und zum guten Schluss darf ich begrüßen Herrn Andreas Könen aus dem BMI, der heute extra für uns seinen 60. Geburtstag unterbricht. Und deswegen darf ich ihm ganz herzlich zum Geburtstag gratulieren. Und, Herr Könen, ich habe in meine Frankenwein-Schatztruhe gegriffen und Ihnen noch einen kleinen Wein mitgebracht von zu Hause.

MD **Andreas Könen** (BMI): Danke sehr.

Vors. **Andrea Lindholz** (CDU/CSU): Wenn Sie sich schon für uns heute bei diesem auch von Ihnen selbst vorhin als sehr wichtig bezeichneten Thema persönlich die Zeit nehmen. Ich könnte jetzt natürlich sagen: Corona – Feiern ist eh nicht. Es ist schöner im Innenausschuss, aber das ist ja auch nicht wirklich so. Also, vielen Dank noch mal, dass Sie da sind.

Es geht heute um das IT-Sicherheitsgesetz, den Gesetzentwurf der Bundesregierung sowie die Anträge der Fraktion der AfD auf der Bundestagsdrucksache 19/26106, den Entwurf der Bundesregierung auf der BT-Drucksache 19/26225 und den Antrag der AfD auf BT-Drucksache 19/26226. Es ist unsere 124. Sitzung, zu der ich heute eröffnen darf, und wir haben ein zweistündiges Anhörungsfenster vorgesehen. Wir wissen jetzt, wer zugeschaltet ist und wer im Raum sitzt. Es wird von der Anhörung wie immer eine Übertragung im Parlamentsfernsehen des Deutschen Bundestages geben sowie die entsprechende Übertragung auf der Homepage des Deutschen Bundestages. Im Anschluss daran ist die Anhörung in der Mediathek abrufbar. Schriftliche Stellungnahmen haben wir erhalten. Ich darf mich dafür ganz herzlich bedanken, auch dafür, dass Sie uns mit Ihrer Expertise alle zur Verfügung stehen. Wir werden im Anschluss an die Sitzung das Protokoll übersenden. Dem Protokoll beigefügt werden dann auch die Stellungnahmen, die aber auch schon versandt worden sind. Das Ganze wird in einer Gesamtdrucksache erfasst. Es wird ein Wortprotokoll angefertigt, das Ihnen allen zur Korrektur übersandt wird. Im Anschreiben werden Ihnen die Details zur Behandlung mitgeteilt. Wenn dann alle mit allem einverstanden sind, wird die Gesamtdrucksache, bestehend aus dem Protokoll und den schriftlichen Stellungnahmen, in das Internet eingestellt.

Zum Prozedere halten wir es bei uns so, dass jeder Sachverständige zunächst die Möglichkeit erhält, ein fünfminütiges Eingangsstatement abzuhalten und wir danach in die Fragerunde der Kolleginnen und Kollegen einschreiten. Weil wir keine Uhr haben, die eingeblendet ist, ich nur meine kleine Uhr immer hier zu Hilfe habe, bitte ich jeden, ein bisschen mit auf die Zeit zu achten und das Fünf-Minuten-Fenster nicht allzu sehr zu überschreiten. Bei den Fragen der Kollegen gilt: In der ersten Fragerunde kann jede Fraktion entweder zwei Fragen an einen Sachverständigen stellen, eine

gleiche Frage an zwei Sachverständige oder an zwei Sachverständige jeweils eine unterschiedliche Frage. Für die zweite Runde werden wir dann entsprechend der noch vorhandenen Zeitdauer entscheiden, wie wir vorgehen. Dass alle Ihre Mikros ausschalten, die selber nicht sprechen, dürfte jetzt Usus sein. Dann würde ich jetzt mit Herrn Artz direkt beginnen und ihn um sein Eingangsstatement bitten.

SV **Sebastian Artz** (Bitkom e. V., Berlin): Ja, sehr geehrte Frau Vorsitzende, sehr geehrte Abgeordnete, meine sehr geehrten Damen und Herren, zunächst möchte ich mich recht herzlich für die Möglichkeit bedanken, heute hier sprechen zu dürfen. Der zur Diskussion stehende Entwurf eines IT-Sicherheitsgesetz 2.0 hat Bitkom in der Ihnen vorliegenden Stellungnahme ausführlich gewürdigt. Zusammenfassend gesagt ist es wichtig und auch richtig, dass sich der Gesetzgeber verstärkt mit den Fragen und Bedarfen der IT-Sicherheit auseinandersetzt. In der Genese des Gesetzestextes ist dies aus Sicht des Bitkom allerdings nur bedingt geglückt und die angedachte Umsetzung ist in wesentlichen Punkten kritisch und überarbeitungsbedürftig. Dabei ist unbestreitbar, dass die Sicherheit von Hardware und Software, aber eben auch der Resilienzaufbau in Kritischen Infrastrukturen zentrale Faktoren sind für den Schutz, die Strahlkraft, aber eben auch die digitale Souveränität des Wirtschaftsstandorts Deutschland. Allerdings dürfen wir gerade in dem Kontext digitale Souveränität nicht als Autarkie verstehen, sondern im Sinne unserer Fähigkeit, selbstbestimmt Entscheidungen zu treffen und neue Technologien vollumfänglich zu durchdringen. Dabei geht es nicht nur, aber natürlich auch um 5G. Wenn wir aber über Technologien wie beispielsweise 5G sowie deren Regulierung sprechen, dann muss ein technologieneutraler Ansatz unser gemeinsamer Ausgangspunkt sein. Denn nur so kann es uns gelingen, dass wir neue Entwicklungen frühzeitig erfassen und faire Bedingungen für alle Unternehmen schaffen. Die vom Gesetzgeber vorgesehene Säule der technischen Zertifizierung kritischer Komponenten geht hier in die richtige Richtung. Einfach, weil die Sicherheit von IT-Produkten und Systemen in erster Linie eine technische und organisatorische Frage ist, die eben genau dann einer regel- und kritikalitätsbasierten Prüfung und Zertifizierung als Antwort bedarf. Im Gegensatz dazu handelt es sich bei der vorgesehenen Säule der Vertrauenswürdigkeitsprüfung um ein politisches Instrument. Das kann zwar sicherheitspolitisch gewollt sein, ist dann aber eben auch rechtssicher auszugestalten und muss klar getrennt von der Säule der technischen Zertifizierung betrachtet werden. Das ist aktuell nicht gewährleistet und daher in der aktuellen Form abzulehnen. Dabei ist sich die Wirtschaft natürlich auch der sicherheitspolitischen Bedeutung des Gesetzesvorhabens gerade mit Blick auf den 5G-Netzausbau bewusst. Deshalb verweisen wir eben auch explizit auf die Notwendigkeit der vollständigen Umsetzung der europäischen 5G-Toolbox. Denn nur ein gemeinsames europäisch abgestimmtes Vorgehen kann aus globaler Wettbewerbsperspektive langfristig zielführend sein. Fakt ist aber auch, dass Sicherheitspolitik üblicherweise ein Invest des Staates ist, das allzu häufig reaktiv erfolgt, also dann, wenn es bereits zu spät ist. Das gilt auch für das IT-Sicherheitsgesetz 2.0, das mehr zurückblickt als gestalterisch und richtungsweisend nach vorne. Das ist insofern bedauerlich, als dass technische Innovationszyklen alle paar Jahre erfolgen und dabei nicht an nationalen Grenzen haltmachen. In fünf Jahren ist es sehr gut möglich, dass wir Unternehmen A aus Land B oder Unternehmen X aus Land Y ganz anders wahrnehmen, einfach, weil sich auch der Stand der Technik weiterentwickelt hat.

Um es in dem Kontext auch einmal ganz klar zu sagen: Der Stand der Technik ist ein volatiles Konstrukt, das sich stetig weiterentwickelt und unter Einbeziehung aller relevanter Stakeholder im Zuge des Normungs- und Standardisierungsprozesses durch technische Regeln beschrieben wird. Ausgangspunkt dafür bilden internationale und europäische Standards und Normen, keine nationalen technischen Richtlinien. Anders als aktuell vorgesehen kann das BSI als nationale Behörde den Stand der Technik also nicht einfach definieren oder festlegen. An dieser Stelle kommt dann eben auch ein zentraler Kritikpunkt des Bitkom zum Ausdruck, nämlich die fehlende Spezifizierung von Schutzzielen. Erst auf Basis eines klaren Verständnisses von Schutzzielen lassen sich begründbar IT-sicherheitssteigernde Maßnahmen ableiten, die dann einer permanenten und vor allem eben auch einer risikobasierten Wirksamkeitsprüfung unterzogen werden, um eben langfristig ein hohes Sicherheits- und Schutzniveau

in Kritischen Infrastrukturen gewährleisten zu können. Im IT-Sicherheitsgesetz 2.0 fehlt leider dieser dynamische Grundgedanke ebenso sehr, wie die zwingend erforderliche Einbindung der Wirtschaft. Im Kern lautet die zentrale Frage daher: Wo soll und wo wird Innovation künftig stattfinden? Anstatt reaktiv die Vergangenheit zu regulieren, bräuchten wir ein IT-Sicherheitsgesetz, das die Wirtschaft eben nicht als Gegner wahrnimmt und die Aufwände und Kosten einseitig abwälzt, sondern ein mutiges IT-Sicherheitsgesetz, das einerseits den Dreiklang aus Innovationsfreundlichkeit, Rechtssicherheit und Investitionsschutz hochhält und andererseits ein vertrauensbasiertes, ein gemeinschaftliches und vor allem eben auch ein europäisches Ökosystem fördert, in dem wir alle gemeinsam an einem Strang ziehen, um die Innovation von morgen in Deutschland und Europa hervorzubringen und den Schutz unserer kritischen Infrastrukturen zu gewährleisten. In der politischen Debatte wird dabei auch allzu häufig übersehen, dass die Wirtschaft aus privatwirtschaftlichen Gründen heraus bereits aktiv daran arbeitet, einseitige Abhängigkeitsverhältnisse zu reduzieren und neue Handlungsalternativen aus eigenen Stücken heraus zu schaffen. Es ist kein Zufall, dass sich die Wirtschaft mit Fragen der Interoperabilität, Open RAN, Netzwerkvirtualisierung, 6G und vielem mehr auseinandersetzt. Das IT-Sicherheitsgesetz 2.0 muss daher zu einem dynamischen Regelwerk entwickelt werden, welches Innovation und Sicherheit gemeinsam mit der Wirtschaft denkt. Was die deutlich zu weit reichenden Anordnungs- und Eingriffsmöglichkeiten von BMI und BSI angeht sowie den intransparenten Umgang mit Schwachstellen, werden die nachfolgenden Sachverständigen ins Detail gehen und Punkte ansprechen, die auch für den Bitkom von zentraler Bedeutung sind. Herzlichen Dank.

Vors. **Andrea Lindholz** (CDU/CSU): Vielen herzlichen Dank, Herr Artz. Wir kommen jetzt zu Herrn Atug, der uns zugeschaltet ist.

SV **Manuel Atug** (AG KRITIS, Bonn): Vielen Dank, Frau Vorsitzende. Meine Damen und Herren, es geht in dieser Anhörung um die Erhöhung der IT-Sicherheit. Dazu haben sich bereits initial in der Analyse des IT-Sicherheitsgesetzes 2.0 zwei Kernpunkte aufgedrängt. Zum einen die augenscheinliche Strategie- und Ziellosigkeit im gesamten bisherigen Verfahren, kombiniert mit der fehlenden Evaluierung des IT-Sicherheitsgesetz 1.0 als ein Beispiel dafür. Zum anderen der offensichtliche Konflikt zur Sichtweise auf die IT-Sicherheit. Über zwei Jahre wurde vor sich hin gewerkelt. Interessierte und Betroffene konnten sich in der Zeit nur durch geleakte Referentenentwürfe informieren. Beteiligung sieht anders aus. Im Dezember letzten Jahres ging es dann Schlag auf Schlag. Fünf Referentenentwürfe innerhalb von wenigen Tagen und zuletzt lediglich 26 Stunden als Frist zur Einreichung einer Stellungnahme zu über 100 Seiten Gesetztext. Beteiligung, meine Damen und Herren, sieht einfach anders aus! Cybersicherheit in Deutschland endet nicht bei den Zuständigkeiten in und um das Bundesministerium des Inneren. Dies gilt es daher dringend auch im IT-Sicherheitsgesetz 2.0 zu beachten. Das IT-Sicherheitsgesetz 2.0 zeigt aufgrund dieser Vorgehensweise starke Defizite auf. Deutlich wird dies an vielen Stellen durch den erwähnten Konflikt zur Sichtweise auf die IT-Sicherheit. Zum einen blicken Sicherheitsbehörden und Nachrichtendienste im Kontext der Befugniserweiterung auf IT-Sicherheit, also beispielsweise durch Staatstrojaner oder durch invasive Eingriffe in IT-Systeme aufgrund der Gefahrenabwehr, im Volksmund auch Hackback genannt, und damit einhergehend auch durch die Verpflichtung des vermeintlich unabhängigen BSI zur aktiven Zurückhaltung von Sicherheitslücken für unbestimmte Zeiträume. Und auf der anderen Seite IT-Sicherheit im Kontext der Erhöhung der Cyberresilienz aus Sicht der Zivilgesellschaft und der Kritischen Infrastrukturen. Denn die Zivilbevölkerung benötigt robuste und widerstandsfähige Versorgung, beispielsweise mit Strom und Wasser, unabhängig von einer steigenden Digitalisierung in den Produktionsanlagen. Eine einfache Regel in der IT-Sicherheit lautet: Das Zurückhalten von Schwachstellen betrifft immer die Zivilgesellschaft, und zwar weltweit, sowie auch die private Wirtschaft und Betreiber Kritischer Infrastrukturen, ebenfalls weltweit. IT-Sicherheit bedeutet daher im Umgang mit Sicherheitslücken ausnahmslos, diese schnellstmöglichst loszuwerden. Im Hinblick auf drohende Folgen dieser Zurückhaltung von Sicherheitslücken oder gar von IT-Systemausfällen aufgrund des invasiven Einwirkens auf IT-Systeme kann das absichtliche Offenhalten oder Zurückhalten von Sicherheitslücken daher in einer Gesamtabwägung niemals angemessen sein. Findet dies in der Gesetzgebung keine Berücksichtigung,

wird der Staat seiner Verantwortung in der IT-Sicherheit Deutschlands nicht gerecht. Untermauert wird besagte Strategie- und Ziellosigkeit darüber hinaus durch die immer noch ausstehende und – nebenbei angemerkt – gesetzlich vorgeschriebene Evaluierung der Wirksamkeit des bereits 2015 eingeführten Gesetzes. Eine Überarbeitung vorzunehmen, ohne den aktuellen Stand zu analysieren und den daraus resultierenden Erkenntnisgewinn als Feedback einzubringen, zeugt von einer grundsätzlichen und prozessbedingt verminderten Qualität durch Kardinalsfehler im Prozessablauf. Durch die fehlende Evaluierung kann beispielsweise nicht nachvollzogen werden, ob die aktuellen Schwellenwerte die vorgegebenen Schutzziele erreichen, denn im Kritis-Sektor Wasser sind derzeit unter 50 von ca. 5.000 Wasserwerken als Kritis-Betreiber eingestuft. Eine Trennung von defensiven Handlungen durch das BSI und den invasiven, offensiven Maßnahmen durch die Sicherheitsbehörden und Nachrichtendienste würde das kontinuierlich bröckelnde Vertrauen in das BSI wieder erhöhen. Hier wurde aber erneut die Chance vertan, das BSI möglichst unabhängig aufzustellen und dadurch die IT-Sicherheit in Deutschland zu erhöhen. Stattdessen wird das BSI immer stärker zum Handlanger oder wahlweise auch zum verlängerten Arm von Sicherheitsbehörden und Nachrichtendiensten. Werden beispielsweise Systeme zur Angriffserkennung gesetzlich gefordert, fehlen die dafür aufzuwendenden Ressourcen im Zweifel bei den Maßnahmen, die aufgrund einer Risikoanalyse der KRITIS-Betreiber dringender nötig gewesen wären. Ein freiwilliges IT-Sicherheitskennzeichen einzuführen, doppelt sich mit der verpflichtenden Umsetzung des EU-Cybersecurity-Act. Ein Nutzen dieser zusätzlichen freiwilligen Kennzeichen erschließt sich darüber hinaus ebenfalls nicht. Das ganze IT-Sicherheitsgesetz 2.0 steht dabei symptomatisch dafür, wie unsystematisch das Thema IT-Sicherheit in Deutschland adressiert wird. Eine übergreifende und strategische Vorgehensweise, die auch Kommunen, Länder, Wissenschaft und Forschung, Bildung, Wirtschaft, Zivilgesellschaft und die Community der Sicherheitsforscher*innen sinnvoll in die Digitalisierung und damit sowohl in die Cybersicherheit als auch in die digitale Souveränität Deutschlands einbettet, fehlt leider völlig. Danke sehr.

Vors. **Andrea Lindholz** (CDU/CSU): Herr Professor Gärditz bitte.

SV **Prof. Dr. Klaus F. Gärditz** (Rheinische Friedrich-Wilhelms-Universität Bonn): Herzlichen Dank, Frau Vorsitzende. Ich möchte hier dezidiert Stellung nehmen nur als Sachverständiger für den Bereich Verfassungs- und Verwaltungsrecht. Ich bin kein IT-Rechtler und möchte also bewusst Schwerpunkte setzen auf vor allem die Regelung des § 9b, die vielleicht so zum politischen Herzstück gehört. Was das Gesetz insgesamt angeht, verfolgt das sachgerechte Ziele. Es versucht, den Rahmen zur Gewährleistung von Netzinfrastruktursicherheit weiter zu verbessern, auszubauen, hat dafür vernünftige Instrumente und begegnet jedenfalls in diesen operativen Regelungen weder verfassungsrechtlichen Bedenken noch verwaltungsrechtlichen – ich sag mal – Applikationsproblemen, die zu erwarten sein werden. Insgesamt kann ich also diese Novelle unterstützen, möchte jetzt aber eine paar kritische Blicke auf den § 9b lenken. Ich bin ja häufiger hier im Innenausschuss. Dass ich aber einmal ein Gesetz hier zur Begutachtung bekomme, was ein dezidiertes Anti-Sicherheitsgesetz ist, ist auch für mich eine neue Erfahrung. Diese Regelung des § 9b, die also den Einbau kritischer Komponenten beim Infrastrukturausbau regeln möchte, verfolgt eigentlich das vernünftige Anliegen, dass man bestimmte Bereiche unserer Infrastrukturen im Interesse der digitalen Souveränität, aber damit letzten Endes unseres gesellschaftlichen Miteinanders gegen Manipulation und Angriffe besonders schützen soll. Diese Regelung ist aber, so wie sie jetzt ausgestaltet ist, weder verfassungskonform noch rechtlich vernünftig operabel. Verfassungsrechtlich – ich habe das in meiner schriftlichen Stellungnahme näher ausgeführt – sehe ich vor allem zwei bzw. drei Kernprobleme. Ganz zentral leidet diese Norm an einer ganz grundlegenden Unbestimmtheit, weil die Eingriffsvoraussetzungen für das BMI bei festgestellten möglichen Defiziten der Vertrauenswürdigkeit völlig konturenlos ausgestaltet sind. Es wird ganz allgemein auf nicht näher konkretisierte politische Ziele verwiesen. Das kann auch die jeweilige tagespolitische Opportunität sein. Das genügt dem Vorbehalt des Gesetzes nicht, weil wir uns hier in einem ganz zentralen grundrechtlichen Bereich bewegen, die Sicherheit unserer Netze, nicht zuletzt der Deka-Netze ist natürlich von kardinaler gesellschaftlicher Bedeutung. Über die

verwirklichen sich Grundrechte, über die findet demokratische Willensbildung statt. Da muss auch das Parlament Verantwortung für die basalen Kriterien von Eingriffen übernehmen. Die Unbestimmtheit dieser Norm führt zudem dazu, dass auch bei Fällen einer Versagung oder Untersagung des Technologieeinsatzes keine rechtlich handhabbaren Kriterien zur Verfügung stehen, so eine Entscheidung wirksam zu überprüfen, weswegen die Bestimmung auch gegen Artikel 19 Absatz 4 Grundgesetz, das Gebot des effektiven Rechtsschutzes, verstößt.

Inhaltlich sehe ich eine ganze Reihe an Defiziten an dieser Norm, die deren Operabilität im konkreten Einsatz in Frage stellen und wo ich mich gefragt habe aus nüchterner verwaltungsrechtlicher Sicht, ob eigentlich irgendjemand ernsthaft mit der Anwendung dieser Norm rechnet. Beispiele, einfach nur, um das zu konturieren, mehr in meinem Papier: Eine Untersagung einer als nicht vertrauenswürdig festgestellten Komponente kann nur innerhalb eines Monats nach einer Anzeige im Einvernehmen mit sämtlichen Ressorts erfolgen. Das heißt, das BMI muss in einem knappen Monat sämtliche Ressorts zum Einvernehmen bewegen, um dann eine auch noch hochkomplexe, vom Sachverstand höchst anspruchsvolle Entscheidung zu begründen und zu erlassen. Das kann nicht funktionieren. Da geht die Norm praktisch ins Leere. Ein zweiter Punkt ist etwa das inadäquate Beweismaß: Unzuverlässigkeit muss ich nachweisen anhand von unwahren Tatsachen in der entsprechenden Herstellererklärung. Nur wird sich solch ein außenpolitisches Risiko einer – ich sag mal – Einflussnahme durch ausländische Staaten und ihre Akteure nie mit einer strafprozessualen Überzeugungssicherheit belegen lassen, sondern im Wesentlichen auf Prognosen und nachrichtendienstlichen Erkenntnissen beruhen. Dieses Beweismaß, die Beweislast, die hier der Bund zu tragen hätte, führt im Effekt dazu, dass diese Norm praktisch nicht zur Anwendung kommen kann. Und wenn ich einem anderen Staat tatsächlich beweisen muss, dass er manipulativ Unternehmen und deren Technologie einsetzt, um unsere Netze angreifbar zu machen, treibt die Begründung eines solchen Verwaltungsaktes uns in die außenpolitische Eskalation.

Insgesamt also leidet die Regelung – weitere Mängel habe ich aufgezeigt – unter erheblichen Defiziten, die sie praktisch inoperabel macht. Damit wird letzten Endes auch der Infrastrukturgewährleistungsauftrag des Art. 87f Absatz 1 Grundgesetz unterlaufen, der nämlich nicht nur die Zurverfügungstellung hinreichend leistungsstarker, sondern auch hinreichend sicherer Netze als eine Aufgabe des Bundes verfassungsunmittelbar ausgestaltet. Insgesamt halte ich es für problematisch, dass der Deutsche Bundestag an Glaubwürdigkeit einbüßt, wenn er einerseits mit Recht immer wieder den verfassungsrechtlich hohen Rang der inneren und äußeren Sicherheit betont und damit auch ggf. notwendige Grundrechtseingriffe rechtfertigt, hier aber eine Placebo-Norm formuliert, die eigentlich nur darauf ausgerichtet ist, die Durchsetzung von Sicherheitsbelangen gegenüber ökonomischen Interessen bestmöglich zu verhindern. Die einseitige Ausgestaltung als eine reine technikrechtliche Bestimmung halte ich zudem ebenfalls für problematisch, denn bei der Frage, mit welchem Staat und wessen Unternehmen wir kooperieren wollen und wo wir Risiken eingehen wollen, ist natürlich auch eine der politischen Systemkompatibilität und es ist natürlich ein Unterschied, ob wir etwa einerseits mit China oder Russland oder andererseits mit Großbritannien oder den USA kooperieren wollen. Das spricht auch dafür, dass der Deutsche Bundestag in eine grundsätzliche Reformulierung der Norm eintreten sollte.

Sollte es am Ende zu einer Änderung kommen, lassen Sie sich bitte nicht von einer Notifizierungsfrist, die eine entsprechende Richtlinie der EU vorsieht, schrecken. Eine solche Notifizierung kann ggf. auch noch nachträglich vorgenommen werden und ist kein Hinderungsgrund, das parlamentarische Verfahren und seine Wirksamkeit aufzuhalten. Machen Sie ein gutes Gesetz, nicht ein eiliges Gesetz. Herzlichen Dank.

Vors. **Andrea Lindholz** (CDU/CSU): Herr Professor Gärditz, vielen Dank. Herr Dr. Herpig bitte.

SV **Dr. Sven Herpig** (Stiftung Neue Verantwortung e. V., Berlin): Ja, liebe Frau Vorsitzende, liebe Abgeordnete, liebe Menschen, die Gefährdungslage im Cyberraum ist laut Bundesamt für Sicherheit in der Informationstechnik nun seit mehreren Jahren weiterhin auf einem sehr hohen Niveau angespannt. Daher begann das Bundesministerium des Innern, für Bau und Heimat vor über zwei Jahren seine Arbeit an einem IT-Sicherheitsgesetz 2.0,

einem weiteren Mosaiksteinchen der deutschen Cybersicherheitspolitik – und es hätte ein Meilenstein werden können. Leider reichte der Vorlauf offenbar nicht aus, damit dieser Gesetzesentwurf den angemessenen Prozess hätte durchlaufen können, der ihm qua seiner Relevanz für die Sicherheitspolitik in Deutschland zusteht. Eine notwendige Teilevaluierung aus dem Vorgängergesetz hätte eine empirische Basis für die Maßnahme im IT-Sicherheitsgesetz 2.0 bilden können, wurde aber kurzerhand gestrichen. Die Einbindung von Wirtschaft, Wissenschaft und Zivilgesellschaft war nur ein Feigenblatt, wie Herr Atug schon eloquent ausgeführt hatte. Der nationale Normenkontrollrat befand entsprechend, dass bei der Vorbereitung dieses Regelungsvorhabens in mehrfacher Hinsicht gegen die Grundsätze besserer Rechtsetzung verstoßen wurde. Beim Gesetzesentwurf, der teils invasive Befugnisse beinhaltet und einen Erfüllungsaufwand von knapp 200 Millionen Euro pro Jahr, und damit eingeschlossen knapp 1.600 Planstellen für die Verwaltung vorsieht, wäre ein anderes Vorgehen angemessen gewesen. Gerade vor dem Hintergrund der nach wie vor herrschenden Knappheit an IT-Sicherheitsfachkräften im öffentlichen Dienst und den wirtschaftlichen Folgen der COVID-19-Pandemie.

Ich möchte an dieser Stelle nur drei Kritikpunkte meiner schriftlichen Stellungnahme vielleicht noch mal herausstellen und zusammenbinden.

Erstens, beim Eingriff der Diensteanbieter in die Integrität von Kundensystemen gemäß § 7c Absatz 1 Satz 1 BSI-G handelt es sich um einen angeordneten Eingriff in das Computergrundrecht. Es ist unklar, wie die operative Umsetzung aussehe und welche Schutzmechanismen greifen würden. Darüber hinaus bietet diese Maßnahme im Sinne der IT- und Cybersicherheit keinen erkennbaren zusätzlichen Schutz zu den bereits bestehenden Maßnahmen, unter anderem das Informieren der Kund*innen und möglicherweise Schutz vor weiteren Schäden durch den Walled Garden. Diese Gesetzesänderung sollte daher ersatzlos gestrichen werden.

Zweitens, es ist schwer verständlich, dass auf der einen Seite relativ breite Befugnisse für die Untersuchung der Informationstechnik der Hersteller durch das BSI geschaffen werden, aber gleichzeitig einzelne behördliche Bereiche von der Untersuchung der Informationstechnik und den Mindeststandards ausgenommen werden sollen und entsprechende Begründungen und Verwaltungsvereinbarungen nicht zwingend öffentlich werden. Während die Ausnahmeregelung für die Bundeswehr unter anderem auf Basis der eigenen IT-Fähigkeiten im Organisationsbereich Cyber- und Informationsraum nachvollziehbar erscheint, ist gerade die Ausnahme des Auswärtigen Amtes unverständlich und ein falsches Signal für die IT-Sicherheit in Deutschland. Aus diesem Grund sollte § 4a Absatz 5 BSI-G ersatzlos gestrichen werden, Absatz 6 müsste in der Begründung umfassender erklärt werden und die Verwaltungsvereinbarungen sollten öffentlich gemacht werden. Da bereits im Rahmen des IT-Sicherheitsgesetzes 1.0 der Ausschuss für Inneres und Heimat 2015 in seiner Beschlussempfehlung das Einvernehmen im damaligen § 8 BSI-G durch das Benehmen ersetzt hat mit der Begründung, dass die Einvernehmenserfordernis die Schaffung eines einheitlichen Mindestsicherheitsniveaus faktisch verhindere, sollte auch die Festlegung der Mindeststandards für die Sicherheit in der Informationstechnik des Bundes durch das BSI mit den Ressorts im Benehmen statt im Einvernehmen erfolgen gemäß § 8 Absatz 1 BSI-G.

Drittens, in der aktuellen Form lässt das Gesetz eine Strategie der Bundesregierung zum digitalen Verbraucherschutz vermissen, denn nach derzeitiger Rechtsprechung und bei Implementierung des vorliegenden Gesetzesentwurfs dürften weiterhin Elektronikgroßhändler unsichere, unpatchbare Geräte ohne expliziten Hinweis darauf verkaufen, aber der Hersteller könnte freiwillig ein Siegel dafür beantragen, das kenntlich macht, wie unsicher sein Gerät eigentlich ist. Auf der anderen Seite soll das BSI aber nicht die Befugnis bekommen, Portscans auf dynamische IP-Adressbereiche durchzuführen und über die Provider die Kund*innen zu warnen, damit diese ihre Heimnetze besser absichern können. Darüber hinaus entsteht für die Implementierung des IT-Sicherheitskennzeichens ein Mehraufwand von dutzenden Planstellen und mehr als einer Million Euro pro Jahr. Aus Sicht der Effizienz ist stark zu bezweifeln, dass der Ertrag den Aufwand hier rechtfertigt. Die Bundesregierung sollte stattdessen darauf hinarbeiten, dass bekanntermaßen unsichere und nicht mehr absicherbare IT-Produkte über-

haupt nicht in den Handel gelangen dürfen. Weiterhin sollten konkrete Maßnahmen ergriffen werden, die direkt für eine höhere Sicherheit der IT-Produkte sorgen, wie zum Beispiel Netzwerksegmentierung in Routern. Der Entwurf des IT-Sicherheitsgesetzes spiegelt leider auch irgendwie die Cybersicherheitspolitik der letzten Jahre wieder. Keine Strategie, keine Evaluierung und eine schlechte Einbindung von Wirtschaft, Wissenschaft und Zivilgesellschaft. Vielen Dank.

Vors. **Andrea Lindholz** (CDU/CSU): Herr Dr. Herpig, vielen Dank. Herr Neumann bitte.

SV **Linus Neumann** (Chaos Computer Club Berlin): Ja, herzlichen Dank, Frau Vorsitzende. Herzlichen Dank an die Ausschussmitglieder. Ich spreche heute zu Ihnen als Vertreter des Chaos Computer Clubs, einer Hacker*innen-Vereinigung, die hier seit mehreren Jahrzehnten in der Bundesrepublik Deutschland ihr Unwesen treibt. Wir machen sowas, wie die Staatstrojaner analysieren oder die Bundestagswahlsysteme hacken, aber wir melden die Schwachstellen immer, um auf die IT-Sicherheit hinwirken zu können. Daher kenne ich auch den Herrn Könen, dem ich natürlich auch herzlich noch mal zum Geburtstag gratulieren möchte heute.

Wenn wir uns die Digitalisierung in Deutschland anschauen, dann haben wir hier einfach mit dem Schlechtesten aus beiden Welten zu tun. Wir kommen kaum in den Genuss der Vorteile, wir können ein Impfsystem nicht koordinieren, wir können die Zusammenarbeit der Gesundheitsämter nicht koordinieren, wir können noch nicht mal eine Remote-Anbindung von Sachverständigen im Innenausschuss herstellen, ohne Probleme zu haben. Aber ohne diese Vorteile überhaupt der Digitalisierung zu haben, haben wir alle Nachteile am laufenden Band. Die Kundendaten landen die ganze Zeit online, die Randsomware grassiert seit Jahren durch die Unternehmen und unsichere Produkte ohne Updates sind frei verkäuflich und niemand tut etwas dagegen. Für die Bundesrepublik Deutschland geht die gesamte Rechnung der Digitalisierung nicht auf. Wir bremsen uns selbst und die Zukunft dieses Landes, weil wir nicht kompromisslos für IT-Sicherheit eintreten. Wir brauchen Mut, Sicherheit und Leuchtturmprojekte. Und das letzte, was wir brauchen, sind Kompromisse oder Bürokratie. Wir tun ja so ein bisschen so, als wäre IT-Sicherheit irgendwie mysteriös. Wir wundern uns, wo die ganze IT-Unsicherheit herkommt und tun so, als könnte man da nichts machen. Aber alle praktisch relevanten Probleme der IT-Sicherheit sind theoretisch längst gelöst. Es gibt nicht irgendwelche Herausforderungen, wo wir nicht wissen, wie wir die bewältigen sollen. Dieses Wissen wird aber nicht umgesetzt, und deswegen ist die praktische IT-Sicherheit ein einziges Desaster. Und wenn es irgendwo ein bisschen brennt, dann braucht man eine Feuerwehr, das ist absolut richtig. Aber wenn es überall brennt, dann braucht man Brandschutz – und das wäre eine solide Basis. Eine solide Basis für die Bundesrepublik Deutschland, der Bürger*innen, Wirtschaft usw. vertrauen können, insbesondere in der Infrastruktur. Was soll man aber machen, wenn das BMI überall rumrennt und Feuer legt?! Wir haben die Ausweitung zur Befugnis des Einsatzes von Staatstrojanern, wir haben die Messenger-Überwachung auf Inhalte, der BND soll Kommunikationsnetzwerke hacken dürfen, die ZITiS wird unterhalten, eine eigene Behörde zur Schwächung von IT-Sicherheit. Und demgegenüber steht das arme, kleine BSI allein auf weiter Flur und muss hinterherfegen und unterliegt auch noch der gleichen Dienstherrin, dem BMI. Statt IT-Sicherheit zu gestalten, muss das BSI IT-Unsicherheit verwalten. Und jetzt soll es auch noch Schwachstellen geheim halten dürfen, und somit verlieren wir dann die halbwegs vertrauenswürdige Institution, die einzige halbwegs vertrauenswürdige Institution, die wir in dem Bereich hatten. Das ist ein herber Verlust für die Bürger*innen.

IT-Unsicherheit ist und bleibt in Deutschland auch viele Jahre nach dem ersten IT-Sicherheitsgesetz ein Marktvorteil. Wir als Chaos Computer Club fordern seit langem eine Produkthaftung. Wir verlangen Mindesthaltbarkeitsdaten, also Updatepflicht als Markteintrittsvoraussetzung. Stattdessen bekommen wir jetzt ein freiwilliges IT-Sicherheitskennzeichen, bei dem die Erfüllung der Anforderungen noch nicht einmal geprüft wird. Das ist wirklich einfach nur eine Wirtschaftsförderungsmaßnahme.

Ich finde das halbwegs in Ordnung, dass das BSI jetzt auch langsam etwas machen darf, was ich seit vielen Jahrzehnten mache, nämlich Portscans. Wenn noch irgendwas am Netz hängt, was so klapprig ist, dass ein Portscan nicht standhält, dann ist das ganz gut, wenn da jemand vorbeikommt, das ist aber eine völlig irrige Annahme,

dass das BSI da schneller als Angreifer*innen vorbeikommen würde. Die prüfen nämlich nicht nur auf Schwachstellen, sondern nutzen sie direkt auch noch aus. Das mit den Portscans habe ich früher auch gemacht, da leide ich seit vielen Jahren unter dem Hackerparagraphen, dessen Revision Sie ja inzwischen vielleicht mal in Angriff nehmen könnten, wenn selbst das BSI nun solche Tools nutzen soll. Ich würde allerdings empfehlen, auf eine Reihe seriöser oder zwielichtiger Anbieter zurückzugreifen, die solche Portscans im Stundenabstand machen und die Ergebnisse online kostenlos bereitstellen oder auch mit Analysefunktionen versehen.

Was mich sehr ärgert ist, dass in einem IT-Sicherheitsgesetz von überwiegenden Sicherheitsinteressen die Rede ist, die das BSI daran hindern sollen, das Wissen über Schwachstellen an Betroffene weiterzugeben. Wie Sie wissen – die sind auch im Gesetzesentwurf erwähnt – gehen die größten Angriffsschäden auf das Geheimhalten von Schwachstellen durch staatliche Stellen zurück. Und das BSI sollte unter keinen Umständen jemals berechtigt sein, bei Kenntnis von Schwachstellen irgendetwas anderes zu tun, als die Betroffenen zu informieren, auf eine Beseitigung der Schwachstellen hinzuarbeiten und zu gegebenem Zeitpunkt die Öffentlichkeit zu warnen. Wir machen im CCC seit vielen Jahren vulnerability disclosure. Und wir werden uns jetzt in Zukunft überlegen müssen, ob wir noch Leute mit gutem Gewissen zum BSI schicken können. Die Maßnahmen zur Entfernung von Schadsoftware – da haben andere sich schon zu geäußert – insgesamt wünschenswert, aber das ist ein schwerwiegender Eingriff mit hohem Risiko, den kann man nicht mal eben auf einer halben Seite hinschreiben, das haben ja auch andere Sachverständige hier schon klar erklärt. Das Ergebnis ist: Schadsoftware ist nicht eng definiert, Information ist zu weit definiert, das Missbrauchspotential ist enorm und dem Schutzziel hier unangemessen. Da erwarte ich einige Ausnutzung dieser Paragraphen, die nicht im Interesse und auch nicht im Sinne derer sind, die das Gesetz so formuliert haben. Zur Beteiligung wurde auch viel gesagt. Ich freue mich, dass Herr Professor Gärditz Ihnen Mut gemacht hat, auch wenn die Notifikationsstillhaltefrist am 18.03. endet, vielleicht trotzdem an diesem Gesetz noch nachzubessern. Vielen Dank für Ihre Aufmerksamkeit.

Vors. **Andrea Lindholz** (CDU/CSU): Herr Neumann, vielen herzlichen Dank. Ich kann ja Ihr Statement bezüglich der Impfgeschwindigkeit und der Vorteile der Digitalisierung teilen. Nicht teilen kann ich allerdings Ihren Einwand, dass man die Schwachstellen der Digitalisierung an Bundestagsanhörungen wie der heutigen Sitzung sehen kann. Es ist bisher die einzige Sitzung, bei der uns am Anfang das Einwählen nicht gelungen ist. Bis jetzt läuft es störungsfrei bei der Bild- und Tonübertragung. Zumindest von unserer Seite. Das wollte ich fürs Protokoll festhalten.

SV **Linus Neumann** (Chaos Computer Club Berlin): Das freut mich sehr für Sie.

Vors. **Andrea Lindholz** (CDU/CSU): Nicht, dass hier der Eindruck entsteht, wir wären hier in einem desolaten Anhörungszustand. Das ist mitnichten der Fall. Ansonsten können wir tatsächlich schneller und flexibler werden. Und auch ich würde es mir wünschen, dass wir manchmal die Digitalisierung etwas besser nutzen könnten.

Herr Schallbruch wäre der Letzte mit seinem Fünf-Minuten-Statement.

SV **Martin Schallbruch** (Digital Society Institute der ESMT Berlin): Frau Vorsitzende, meine Damen und Herren Abgeordneten, erst mal auch von meiner Seite herzlichen Glückwunsch an Sie, lieber Herr Könen, zum Geburtstag. Ich möchte mich herzlich bedanken, dass ich die Gelegenheit habe, hier Stellung zu nehmen. Seit dem Inkrafttreten des ersten IT-Sicherheitsgesetzes 2015 hat sich die Cybersicherheitslage deutlich verschlechtert. Der BKA-Lagebericht für 2019 oder auch der BSI-Lagebericht für 2020 zeigen das deutlich. Straftaten gegen Bürgerinnen und Bürger, Kritische Infrastrukturen, kleinere und mittlere Unternehmen oder auch Angriffe gegen die Bundesverwaltung haben wir in den letzten Jahren sehr häufig gesehen. Mit dem IT-Sicherheitsgesetz hat sich die Situation im Bereich der Kritischen Infrastrukturen deutlich verbessert. Auch das BSI hat seine Arbeit in den letzten Jahren sehr stark ausweiten können. Wir erleben aber gleichzeitig eine Veränderung in der Abhängigkeit von der Informationstechnik und der Komplexität der Informationstechnik. Gleichzeitig ist die IT-Sicherheit zum Gegenstand geopolitischer Auseinandersetzungen geworden. Der Angriff auf amerikanische Stellen, auch einige Stellen in Deutschland, mit Hilfe von

manipulierter SolarWinds-Software durch mutmaßlich russische Stellen oder auch die chinesische Strategie aggressiver Technologiepolitik kombiniert mit Cyberangriffen zeigen diese geopolitische Bedrohung. Es gibt also gesetzgeberischen Handlungsbedarf bei der Sicherheit der Bundesverwaltung, der Sicherheit der Wirtschaft, bei der Produktsicherheit. All das greift der Gesetzentwurf auf und ist insofern eine gute Grundlage für die Beratung im Deutschen Bundestag.

Ich habe in meiner Stellungnahme einige Punkte herausgehoben, die ich wichtig finde für die Diskussion im Bundestag und bei denen weitere Verbesserungen sinnvoll sind.

Erstens, die Sicherheit der Bundesverwaltung: Das BSI hat im Bereich der Bundesverwaltung teilweise geringere Befugnisse als im Bereich der Kritischen Infrastrukturen. In letzter Runde – das hatte Herr Herpig eben schon angesprochen – haben die Ressorts dem BSI die Möglichkeit genommen, Mindestsicherheitsnormen festzulegen, haben sich ein Vetorecht gesichert. Das, glaube ich, sollte das Parlament korrigieren.

Zweitens, das Konzept zum Schutz der deutschen Wirtschaft durch das IT-Sicherheitsgesetz 2.0 ist aus meiner Sicht noch kein ausgewogenes Konzept. IT-Sicherheit in der Wirtschaft wird nicht dadurch erreicht werden, dass das BSI jedes System in einem deutschen Unternehmen kontrolliert, sondern dadurch, dass wir Mechanismen vertrauensvoller Zusammenarbeit aufbauen. Es spricht viel für die Einbeziehung weiterer Bereiche der Wirtschaft. Aber das sollte keine undifferenzierte Einbeziehung der größten Unternehmen völlig unabhängig von der Art der IT, völlig unabhängig vom Schutzziel sein. Sozusagen vom iPad des Pförtners bis zur Produktionsanlage. Das ist auch europäisch nicht anschlussfähig. In Europa hat die EU-Kommission einen Entwurf vorgelegt, der eine Erweiterung entlang von Branchen wie bei Kritischen Infrastrukturen vorsieht. Das deutsche Konzept an dieser Stelle ist aus meiner Sicht verfehlt. Gleichzeitig wird den Unternehmen wenig Mehrwert durch die erweiterten Befugnisse des Staates zurückgeliefert. So etwas wie eine Überprüfung von Administratoren auf Vertrauenswürdigkeit. Oder so etwas wie eine Unterrichtungspflicht durch das BSI über gefundene Schwachstellen und Sicherheitslücken wären sinnvoll, um das Schutzkonzept zugunsten der Wirtschaft zu erweitern.

Drittens, Produktsicherheit: Es ist gut, dass die kritischen Kernkomponenten in einem § 9b gesondert geregelt werden. Das ist ein wichtiger Bereich unserer Infrastruktur, bei dem IT-Sicherheit gewährleistet werden muss. Auch der Ansatz der technischen Zertifizierung ist gut und auch der Gedanke, dass wir zusätzlich eine sicherheitspolitische Vertrauenswürdigkeit der Hersteller brauchen. Was nicht so gelungen ist, ist die Verknüpfung der Zertifizierung und sicherheitspolitischen Entscheidung in einem Verwaltungsverfahren. Das halte ich ähnlich wie Herr Gärditz für praktisch untauglich – alleine die 30-Tage-Frist ist völlig ungeeignet. Die komponentenbezogene Durchführung eines Verwaltungsverfahrens ist unpolitisch und schränkt den Handlungsspielraum der Bundesregierung, beispielsweise mit unseren Verbündeten in EU und NATO gemeinsam zu agieren, enorm ein. Ich würde diese beiden Aspekte – technische Zertifizierung und sicherheitspolitische Belange im Hinblick auf einen Hersteller – voneinander trennen und letzteres, beispielsweise wie bei Rüstungsexporten, dem Bundessicherheitsrat überantworten.

Viertens, technische Vorgaben für IT-Systeme sollte der Staat nach Möglichkeit nur in einem engen Umfang machen. Solche Vorgaben werden am Markt gebildet. Ich unterstütze die Aussagen von Herrn Artz, dass wir hier eine dynamische Regulierung brauchen. Es ist falsch, wenn das BSI den Stand der Technik vorsieht und festlegt. Es ist ebenso schlecht, wenn man durch die Verordnungsermächtigung in § 10 Absatz 6 BSI-G alle Technik in Deutschland durch staatliche Vorgaben standardisiert. Das wird unsere Innovation behindern und der Sicherheit nicht nützen. Ich glaube, wenn man diese Punkte im Gesetzgebungsverfahren aufgreift, werden wir ein deutlich besseres Gesetz für die IT-Sicherheit in Deutschland bekommen. Vielen Dank.

Vors. **Andrea Lindholz** (CDU/CSU): Ja, Herr Schallbruch, auch noch Ihnen vielen herzlichen Dank. Wir kommen dann zur Fragerunde, beginnen mit der Union und hier Herrn Bernstiel bitte.

BE Abg. **Christoph Bernstiel** (CDU/CSU): Sehr geehrte Frau Vorsitzende, werte Kolleginnen und Kollegen, liebe Sachverständige, erst mal vielen Dank an die Sachverständigen, dass Sie sich die

Zeit genommen haben, heute hier mit Ihrer Expertise diesen Gesetzentwurf zu bewerten. Jetzt haben wir einiges gehört. Und ich muss natürlich erst mal vorweg stellen, dass der Gesetzentwurf in Gänze nicht so schlecht ist, wie er hier dargestellt wurde oder wie der eine oder andere vermuten möchte. Man merkt aber auch, dass das Parlament hier selbstbewusst seine Verpflichtung wahrnimmt, auch Entwürfe unsere Regierung zu hinterfragen. Das machen wir hier. Und dazu gibt es ja jetzt auch noch Zeit. Zum Thema Zeit möchte ich auch sagen, dass diese verkürzte Anhörungsfrist, die hier kritisiert wurde, natürlich kann man das machen, aber es ist auch so, dass die Entwürfe dieses Gesetzes schon sehr, sehr lange kursiert sind und dass im letztendlichen Referentenentwurf nur noch Details geändert wurden und für uns die Frage auch stand: Wollen wir diesen Gesetzesentwurf in dieser Legislatur auch noch über die Bühne bringen, ja oder nein? Und Sie hatten es angesprochen, die EU-Notifizierung hat es natürlich erforderlich gemacht, diese drei Monate Zeit einzubauen. Also, wenn der eine oder andere überfordert wurde, dann tut mir das natürlich leid, aber grundsätzlich geht es jetzt darum, diesen Gesetzesentwurf auch durchbringen. Und ich denke, vieles war bekannt.

Ich möchte auch noch etwas sagen zu dieser Aussage, das BMI würde Feuer legen. Das weise ich natürlich direkt zurück. Das BMI legt kein Feuer, sondern das BMI ist zusammen mit den Behörden, die ihm unterstellt sind, einer der maßgeblichen Garanten, die IT-Sicherheit in unserem Land voranzubringen. Und wenn es denn so wäre, wie wir uns das alle wünschen würden, dass sich die IT-Sicherheit in unserem Land selbst regulieren würde, dann bräuchten wir so ein Gesetz nicht. Die Erfahrung zeigt uns aber, dass es leider nicht so ist, sondern dass es nach wie vor sehr viele Lücken gibt, sehr viele ungeregelte Bereiche, und da muss eben der Gesetzgeber und müssen wir als Parlament einschreiten, um dort das Niveau der IT-Sicherheit in Gänze zu heben. Das wird das IT-Sicherheitsgesetz allein natürlich nicht schaffen, aber es ist ein guter Ansatz.

Jetzt zu den konkreten Fragen. Wir werden das auch so teilen, die zweite Fragerunde, also ich würde schon mal ankündigen, dass es eine gibt, die macht dann mein Kollege Amthor. Jetzt erst mal an Herrn Schallbruch: Es wurde ja jetzt genannt, dass das BSI möglicherweise aus dem BMI herausgelöst werden soll und dass es eine Sicherheitslücke wäre, wenn man das BSI mit zusätzlichen Kompetenzen ausstattet und dann weiterhin im BMI hält. Da würde ich Sie gerne mal um Ihre Einschätzung bitten. Dann der zweite Punkt: Es wurde gesagt, dass Schwachstellen bewusst offengehalten werden, nicht weitergemeldet werden und dass dies sozusagen ein bewusstes Agieren – so habe ich das hier gerade aufgenommen – der Bundesregierung sei, um damit die Cybersicherheit zu gefährden. Da würde ich Sie auch um eine Einschätzung bitten. Das waren schon die zwei Fragen? Okay, dann lassen wir es erst mal bei denen. Danke.

Vors. **Andrea Lindholz** (CDU/CSU): Es waren zwei Fragen an Herrn Schallbruch, korrekt? Gut. Wie schnell wir sind und ob wir eine, zwei, drei Fragerunden machen können, hängt davon ab, wie lange der Einzelne für die Fragen braucht und wie viel Zeit dann wiederum die Antworten in Anspruch nehmen und ob wir dann noch Zeit haben. Jetzt kommt die AfD. Frau Cotar bitte.

BE Abg. **Joana Cotar** (AfD): Ja, vielen Dank an alle Sachverständigen. Die Kritik an dem Gesetz war ja eher vernichtend. Ich hoffe, die Koalition nimmt sich das zu Herzen und überarbeitet diesen Entwurf noch mal ganz gründlich. Meine ersten Fragen gehen an Herrn Atug. Herr Atug, danke dafür, dass Sie die fehlende Evaluierung angesprochen haben. Genau das fordern wir ja in unserem Antrag, aber es ist wie bei viele Gesetzen: Zuerst wird gehandelt und erst danach darüber nachgedacht, was überhaupt Sinn macht. Meine erste Frage dreht sich jetzt aber um die Lex Huawai. In Ihrer Stellungnahme schreiben Sie, Resilienz darf nicht auf dem Verbot einzelner Hersteller basieren. Warum ist das Ihrer Meinung nach so? Resilienz soll durch das Gesetz ja nicht ausschließlich mit dem Verbotsinstrument geschaffen werden, sondern in Kombination mehrerer Instrumente. Warum darf ein Verbot Ihrer Meinung nach nicht sein?

Ich habe noch eine zweite Frage, die dreht sich um das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe. Sie bedauern in Ihrer Stellungnahme, dass das nun doch nicht dafür vorgesehen ist, auch für IT-Katastrophen Krisenreaktionspläne auszuarbeiten. Sehen Sie das BBK in seiner derzeitigen Ausrichtung überhaupt in der Lage, an IT-Themen anzudocken? Und wie bewerten Sie in

diesem Zusammenhang zum Beispiel die Funktionalität der NINA-Warn-App des BBK oder die BBK-LÜKEX-Übung? Danke schön.

Vors. **Andrea Lindholz** (CDU/CSU): So, dann kommen wir jetzt zu Herrn Hartmann.

BE Abg. **Sebastian Hartmann** (SPD): Sehr geehrte Frau Vorsitzende, wie der Kollege Bernstiel möchte ich eins, zwei Vorbemerkungen machen und dann natürlich zu zwei Fragen an zwei Sachverständige kommen.

Vors. **Andrea Lindholz** (CDU/CSU): Das bedeutet, jeder Sachverständige eine Frage.

BE Abg. **Sebastian Hartmann** (SPD): Ja, verstanden. Also, ich glaube natürlich nicht, dass es nur an der technischen Überprüfung lag. Wir erinnern uns ja leider auch als Deutscher Bundestag daran, dass wir in einer Verantwortung waren, die Hardware teilweise zu tauschen und dass es also auch erhebliche Zwischenfälle unserer IT-Infrastruktur geben konnte. Also so abstrakt ist das nicht. Und es hat nicht nur mit einer Tonübertragung zu tun. Die zweite Anmerkung ist natürlich auch: Unabhängig davon, wie lange das BMI für vier oder fünf oder drei Referentenentwürfe braucht, wird sich der Bundestag die Zeit nehmen müssen und insbesondere unser Ausschuss, dann tatsächlich aus diesem Gesetz auch etwas Beschlussfähiges zu machen. Und darum kommt dieser Anhörung auch eine erhebliche Bedeutung zu. Und ich halte es für ausdrücklich auch angezeigt, dass gerade die Sachverständigen uns eine kritische Würdigung dieses Gesetzes ermöglichen, damit wir auch erkennen und noch mal zusätzlich Argumentationen bekommen, wo Änderungsbedarf ist, denn kein Gesetz verlässt den Bundestag so, wie es in den Bundestag eingebracht worden ist. Und darum – das vorweggeschickt – haben wir natürlich auch gerade schon mit hohem Interesse – das sage ich auch für den Koalitionspartner SPD – den seitens der Union benannten Sachverständigen, der eine Rechtswürdigung gemacht hat, Professor Gärditz, vernommen, der ja fast, ich würde es nicht als Totalabriss bezeichnen, aber den § 9b schon in seinen Grundfesten erschüttert hat. Das muss man mal so deutlich festhalten. Und das beim unionsgeführten Haus in der CSU – das habe ich so in einer Anhörung auch noch nicht erlebt, und ich habe die Berichterstattung auch der Infrastrukturabgabe wie die PKW-Maut, die ist auch noch in Erinnerung, das sage ich nur mal hier.

Vors. **Andrea Lindholz** (CDU/CSU): Wir haben jetzt eine Anhörung. Bitte. Wir können jetzt noch zehn Minuten Statements austauschen.

BE Abg. **Sebastian Hartmann** (SPD): Frau Vorsitzende, ich nehme mir das gleiche Recht wie der Kollege Ihrer Fraktion, Bernstiel. Und jetzt komme ich zu den zwei Fragen. Aber es sollte hier auch eine Einleitung sein, weil wir diese kritische Würdigung auch vernommen haben. Dann möchte ich die erste Frage an Herrn Artz von Bitkom richten. Sie haben ja den kooperativen Ansatz in der IT-Sicherheit immer wieder auch in Ihrer Stellungnahme betont. Also die Kooperation zwischen Wirtschaft auf der einen Seite und dem Staat auf der anderen Seite, auch mit dem Ziel des Verbraucherschutzes. Sie haben Ausführungen gemacht zu der Vertrauenswürdigkeitsprüfung im § 9b, dass dieser rechtssicher verfasst muss, sodass er einerseits anwendbar ist, auf der anderen Seite aber auch für die Unternehmen belastbar ist. Da gibt es ja Fragen von den Haftungsregeln bis zu den Fragen der vollständigen Umsetzung der EU-Toolbox mit dem Blick auf 5G. Können Sie das bitte auch aufgrund der vorhandenen Stellungnahmen oder der Ausführungen Ihrer Kollegen, der Sachverständigen, noch mal konkretisieren, wie Sie sich das vorstellen, wie man einen solchen § 9b gestalten könnte, dass er einerseits anwendbar ist, dass er rechtssicher ist und dass er natürlich auch den Zielen des Deutschen Bundestages insofern Rechnung trägt?

Die zweite Frage möchte ich an Herrn Dr. Herpig von der Stiftung Neue Verantwortung richten. Sie haben in Ihrer Stellungnahme, in der letzten Stellungnahme, ausgeführt, dass es ganz zentral ist, auch eine entsprechende Stellung des BSI im Gefüge auf Seiten des BMI, auf Seiten der Bundesbehörden darzulegen. Und zwar geht es einher, dass Sie da einen Bezugspunkt herstellen zwischen der Stellung dieses so entscheidenden Amtes, auf der anderen Seite aber auch mit der Erweiterung der Kompetenzen. Können Sie das am Beispiel des Schwachstellenmanagements mal erläutern, wie man ein solches BSI aufstellen sollte. Dass es auf der einen Seite die Kompetenzen und die personellen Ressourcen hat, aber auf der anderen Seite auch seitens des Gesetzgebers klare Vorgaben, um der Rolle gerecht zu werden, um möglicherweise Interessenkonflikte auszuschließen? Wie muss ein

Gesetz an dieser Stelle formuliert sein, um die Stellung des BSI so unabhängig, so organisatorisch selbstständig aufzustellen, dass es dieses Ziel ohne einen Interessenkonflikt ausführen kann? Danke.

Vors. **Andrea Lindholz** (CDU/CSU): So, Herr Höferlin bitte.

BE Abg. **Manuel Höferlin** (FDP): Vielen Dank, Frau Vorsitzende. Auch ich muss eine Vorbemerkung machen. Es ist schon beachtlich, muss ich sagen, wenn die gesamte Runde der Sachverständigen inklusive der Sachverständigen der Koalitionsfraktionen fundamentale Kritik an einem Gesetz haben, das so lang in der Vorbereitung war und auf das wir so lang gewartet haben. Ich sage nur, Stichworte wie „Anti-Sicherheitsgesetz“ sind gefallen oder „praktisch untauglich“, „politisch enorm einschränkend“, und zwar von Sachverständigen der Koalition. Allerdings habe ich jetzt auch verstanden, Herr Bernstiel, wenn Sie sagen, dass es grundsätzlich – so Ihre Worte – darum geht, dieses Gesetz noch in dieser Legislatur durchzubringen. Und ich dachte, es geht um IT-Sicherheit. Aber lassen wir das.

Ich finde, dass das IT-Sicherheitsgesetz in der Form, wenn es um IT-Sicherheit gehen soll, und das sollte ja im Kern sein, für mich eine Enttäuschung auf ganzer Linie ist in ganz vielen Punkten. Das kann ich leider nicht anders sagen. Es sind viele Reformen nicht vorangekommen. Und am schlimmsten finde ich neben der Geschichte § 9b – ich glaube, die ist gerade heute gestorben nach den Einleitungen, da müsste was nachgearbeitet werden – finde ich den schlimmsten Punkt, dass die Gefährdung der Sicherheitslage, der Cybersicherheitslage durch das ungenügende Sicherheitslücken- oder Schwachstellenmanagement. Und das ist mehrfach hier zu Worte gekommen, deswegen möchte ich auch die zwei Fragen an den Sachverständigen Herrn Dr. Herpig richten. Und zwar geht es genau um den Punkt. Der Gesetzentwurf sieht ja jetzt keine Meldeverpflichtung für Bundesbehörden für gefundene oder erworbene Schwachstellen vor, zum Beispiel an das BSI, und macht zwar Vorgaben für Mindeststandards der IT-Sicherheit von Stellen des Bundes. Diese haben aber für Verfassungsorgane nur empfehlenden Charakter. Vielleicht können Sie kurz ausführen: Wie müssten Meldepflichten, Mitwirkungspflichten oder -befugnisse des BSI Ihrer Ansicht nach gestaltet sein, um tatsächlich dem Ziel der Stärkung der Cybersicherheit näherzukommen. Der zweite Punkt. Den Meldepflichten der verpflichteten Unternehmen stehen ja nur sehr vage Pflichten des BSI gegenüber. Einen echten Rückkanal für zumindest tagesaktuelle Informationen zur Bedrohungslage oder Hilfestellung des BSI für Unternehmen gibt es ja nun nicht wirklich. Sie beschreiben zum Beispiel die Wichtigkeit von Mobile Incident Response Teams. Welche Rückkanäle in die Wirtschaft oder die betroffenen Behörden sollte das BSI denn aufbauen, sollten im IT-Sicherheitsgesetz 2.0 vorgesehen werden, damit am Ende die Bundesregierung nicht zum größten Risiko für die IT-Sicherheit in Deutschland wird?

Vors. **Andrea Lindholz** (CDU/CSU): Herr Höferlin, vielen Dank. Dann Frau Pau bitte.

BE Abg. **Petra Pau** (DIE LINKE.): Ja, danke, Frau Vorsitzende. Und danke an die Sachverständigen. Ich verkneife mir jetzt jede Stellungnahme zu den Stellungnahmen der Kolleginnen und Kollegen und komme gleich zu meinen zwei Fragen an Herrn Atug. Das erste ist ein Thema, das sich hier sich jetzt auch durchzog: das Thema Zurückhalten von Sicherheitslücken. Ich bezweifle ja grundsätzlich, dass das für die Aufgabenerfüllung der Sicherheitsbehörden tatsächlich erforderlich ist und sehe das eher als Gefährdung sowohl der Sicherheit, aber eben auch der Nutzerinnen und Nutzer.

Vors. **Andrea Lindholz** (CDU/CSU): Vielleicht können die Kollegen der Union ihr Zwischengespräch einstellen, denn ich höre es fast bis hier vorne und würde gerne Frau Pau verstehen, auch fürs Protokoll.

BE Abg. **Petra Pau** (DIE LINKE.): Ich wüsste gern von Ihnen, Herr Atug, wie Sie sich ein Schwachstellenmanagement vorstellen, das die IT-Sicherheit tatsächlich für alle erhöht und gesetzlich geregelt werden muss? Und vielleicht können Sie auch praktisch darstellen, was das für die Anwenderinnen und Anwender heißt, also nicht auf der Seite der Sicherheitsbehörden, sondern für uns alle. Und die zweite Frage: Sie haben sich zum BSI kritisch geäußert als nachgeordnete Behörde des Bundesinnenministeriums und schlagen die fachliche Unabhängigkeit in Ihrer Stellungnahme vor. Können Sie uns noch mal kurz sagen, welche Probleme Sie in der aktuellen Konstellation sehen und wie sich diese verschärfen durch die vorgeschlagenen gesetzlichen Regelungen und wie Ihre

Alternative aussehen würde? Danke.

Vors. **Andrea Lindholz** (CDU/CSU): Frau Pau, vielen Dank. Dann ist für Fraktion BÜNDNIS 90/DIE GRÜNEN zuschaltet Frau Rößner.

Abg. **Tabea Rößner** (BÜNDNIS 90/DIE GRÜNEN): Ja, und es klappt hoffentlich auch, weil ich habe nämlich lange gebraucht, um mich einwählen zu können. Vielen Dank, Frau Vorsitzende und vielen Dank für die Stellungnahmen. Ja, eine Vorabbemerkung kann ich mir nicht verkneifen, nämlich dass die Sachverständigen doch durchweg alle ziemlich kritisch sind, was dieses Gesetz angeht. Und ich muss sagen, das ist ja schon fast eine verheerende Kritik für dieses Gesetz und ich denke auch, dass wir einen viel proaktiveren Ansatz bräuchten zur Stärkung der IT-Sicherheit, also Beratung durch unabhängige Behörden und Investitionen in gute IT-Sicherheitslösungen, Auditierung, Zertifizierung usw., statt Unternehmen noch zu bestrafen, wenn sie Opfer eines Angriffs werden.

Meine Fragen richten sich an Linus Neumann, und zwar einmal den Blick ein bisschen geweitet auf die IT-Sicherheitspolitik der Bundesregierung insgesamt. Was bringt denn das IT-Sicherheitsgesetz 2.0, wenn man gleichzeitig eben mit Sicherheitslücken handelt, den Staatstrojaner auf den Geheimdienstbereich ausweitet, an der Vorratsdatenspeicherung festhält, Kryptographie immer wieder in Frage stellt und den Kryptowar nur befeuert, öffentlich über Backdoors in allen IoT-Geräten siniert? Was bedeutet das alles für die Pläne für die IT-Sicherheit? Und wenn das Innenministerium sozusagen das Problem ist und weniger die Lösung, müssten nicht auch diese digitalpolitischen Grundsatzentscheidungen endlich getroffen werden, um im Bereich der IT-Sicherheit vom Fleck zu kommen? Und die zweite Frage bezieht sich auch auf die Meldepflichten. Wie bewerten Sie, dass man selbst bei Unternehmen eben sehr weitreichende Verpflichtungen macht, beispielsweise das Melden von Sicherheitslücken, aber gleichzeitig eben nicht vor der eigenen Haustür kehrt, es bis heute eben keine staatliche Meldepflicht für Sicherheitslücken und kein Schwachstellenmanagement gibt? Und wie müssten die aussehen? Vielen Dank.

Vors. **Andrea Lindholz** (CDU/CSU): Frau Rößner, vielen Dank. Wir kommen dann jetzt zur Beantwortung der Fragen. Nicht, dass Sie mich missverstehen, natürlich können Sie Zwischenbemerkungen machen. Mir ging es nur um die Länge. Ich finde nämlich die Antworten auf die Fragen und Ihre Fragen noch spannender. Also, Herr Artz, mit Ihnen fangen wir an.

SV **Sebastian Artz** (Bitkom e. V., Berlin): Gut, ich beziehe mich direkt auf die Frage von Herrn Hartmann bezüglich der Haftung, aber eben auch den kooperativen Gedanken. Es ist sicherlich, auch in Anbetracht der Anmerkungen der Abgeordneten. noch mal anzumerken, dass gerade der Prozess zum IT-Sicherheitsgesetz 2.0 zum vorliegenden Entwurf etwas steinig war und dass wir hier natürlich ein Stück weit dann auch das Momentum des Abwägens und des Innehaltens vermisst haben, um gemeinsame Diskursräume zu nutzen und die Wirtschaft entsprechend einzubinden. Das ist natürlich dahin gehend auch zu beurteilen, dass wir mit der Garantieerklärung und dem Begriff der Vertrauenswürdigkeit aktuell einen unbestimmten Rechtsbegriff vorliegen haben, der eben einfach eine Negativdefinition darstellt. Das heißt, wir haben zusätzlich im § 9b keine strategischen, sondern technische Kriterien aufgelistet, wenn es um das Thema Vertrauenswürdigkeit geht. Das bedeutet aber, wenn wir beispielsweise die Mathematik zu Rate ziehen, dass eine Negativdefinition nie vollständig sein kann und dass da eben dann die Rechtsunsicherheit herrührt. Das würde bedeuten, dass man hier ein Stück weit dann die Logik umkehren und eine Positivdefinition wählen müsste, um die Vorgaben der 5G-Toolbox entsprechend technischer und strategischer Maßnahmen umzusetzen und dann diese beiden Säulen ganz klar voneinander zu trennen. Also, dass wir einerseits die technische Zertifizierungsperspektive haben und dann, wenn es politisch gewollt ist, diese sicherheitspolitische Vertrauenswürdigkeitsprüfung. Fakt ist aber definitiv, dass entsprechend Rückbauanordnungen nicht in der aktuell vorgesehenen Form durchführbar sind, ohne die entsprechenden Unternehmen anzuhören. Wir brauchen Übergangsfristen. Wir müssen auch ein Stück weit natürlich weiter denken als das. Das heißt, wenn wir uns beispielsweise Vergleichsfälle aus dem Bereich des Automobilsektors anschauen – Thema Abwrackprämie –, aber eben auch die Energiewende, wo Sicherheitsprämien ausgelobt werden

könnten, um eben dann zum Beispiel Technologieübergänge zu nutzen und da natürlich dann ein Stück weit besser dieses Maß zu finden oder auch zu differenzieren zwischen Effektivität und Effizienz. Aktuell wird da sicherlich noch keine ausreichende Balance gewährleistet. Das vielleicht an der Stelle zu der Haftungsregelung und zur notwendigen Ausgestaltung des § 9b, um den Unternehmen einerseits Investitionsschutz zu gewährleisten, aber eben auch die Rechtssicherheit nach vorne gerichtet an die Hand zu geben.

Vors. **Andrea Lindholz** (CDU/CSU): Herr Artz, vielen Dank. Herr Atug.

SV **Manuel Atug** (AG KRITIS, Bonn): Ja, vielen Dank. Vielleicht eine kurze Anmerkung an Herrn Bernstiel, weil er sagte, das Gesetz ist nicht so schlecht, wie es hier dargestellt wurde. Ich möchte dazu nur sagen: Wir Sachverständige alle gesamt haben es kritisiert, und zwar allesamt. Insofern mag es vielleicht auch an den Sachverständigen liegen, diesen Sachverstand kommuniziert zu haben.

Ich komme zu der Beantwortung der Fragen. Es war die Frage: Lex Huawei – warum die Resilienz sich nicht auf das Verbot einzelner Hersteller beziehen sollte. Naja, also die Frage, die sich da stellt ist: Was ist das Ziel der Zertifizierung von kritischen Komponenten? Ich arbeite seit über 23 Jahren in und mit Kritischen Infrastrukturen zusammen und versuche, das weltweit umzusetzen. Ich habe das also wirklich von Nordamerika über Europa, Israel, Kasachstan, Ural, Sibirien, weltweit einmal überall kennengelernt, was das bedeutet. Und damit auch verschiedene Sichtweisen. Und Zertifizierungen sind natürlich auch immer unterschiedliche Blickwinkel, Formen und Farben und Arten. Mit einer Zertifizierung, so wie sie für die kritischen Komponenten erklärt wird, kann man das Einschmuggeln einer Sicherheitslücke durch einen fremden Nachrichtendienst nicht vermeiden. Die Frage ist also, welche Hoffnung soll eigentlich damit verbunden werden und was soll genau verhindert werden? Welche Resilienz will man dadurch erhöhen? Weil es ja eher danach klingt, dass man genau das vermeiden möchte. Auf der anderen Seite stellt sich aber die Frage, wie die Aufrechterhaltung von kritischen Geschäftsprozessen aussehen soll, wenn beispielsweise das BMI den Einsatz untersagt, ja? Wie kann dann die Vermeidung von Versorgungsengpässen oder Ausfällen kritischer Infrastrukturen durch KRITIS-Betreiber eigentlich gewährleistet werden? Der Gesetzesentwurf sieht ja explizit die Untersagung vor oder sogar einen Rückbau von verbauten Komponenten als Anordnung. Also im Endeffekt kann da durch Regulierung politisch motivierter Art die kritische Infrastrukturversorgung der Zivilbevölkerung lahmgelegt werden. Und das ist eine unnötige Gefährdung. Und wenn man sagt, man will diesen Passus eigentlich gar nicht nutzen, der ist irgendwie für den schlimmsten anzunehmenden Fall. Wir fabrizieren damit den schlimmsten anzunehmen Fall! Ich halte das für eine sehr gefährliche Wahrnehmung, wenn wir eine solche Funktionalität in die Gesetzeslage reinsetzen und diese Option ziehen könnten.

Zur zweiten Frage, das BBK, wie es derzeit für digitale Themen aufgestellt ist? Ja, nö, ist es halt nicht. Wo und wie denn auch, ja? Beispielsweise die Idee, das Cyberhilfswerk, was die AG KRITIS als Konzept vorgestellt hat, ist ja bisher auch nicht vom BMI aufgegriffen worden, ob man das für oder mit dem BBK oder dem THW oder allein umsetzt. Cyber hat offenbar in den Umfeldern BBK und THW nichts zu suchen und man möchte Katastrophenschutz und Katastrophenhilfe, ja, anscheinend separat betrachten. Vielleicht möchte man es auch zukünftig mit einer Grundgesetzänderung zusammenführen, die man ja auch für die invasiven Maßnahmen von Sicherheitsschwachstellen Zurückhaltung als auch Einwirkung auf Systeme generieren möchte. Und in diesem Doppelpack könnte man das natürlich wunderbar da reinverheiraten. Allerdings halte ich auch das für eine gefährliche Vorgehensweise. Insofern bräuchte es da einen echten evaluierten und sinnvollen und strukturierten Ansatz, wo nicht nur Sachverständige und Experten angehört werden, sondern auch das, was da angehört, in die Gesetzeslage, vielleicht auch in die Grundgesetzänderungslage reinkommt. Das würde zumindest der digitalen Souveränität als auch der Cybersicherheit Deutschlands sicherlich mal guttun, da eine Struktur und eine Strategie hinter zu haben.

Dann gab es noch die Anmerkung zum BBK: Was ist mit der NINA-App und LÜKEX-Übungen? Also, die NINA-App ist ein Teil von dem sogenannten MoWaS-Warnsystem in Kombination mit einem noch ausstehenden, aber durch die EU sowieso verpflichtend einzuführenden Cellbroadcasting ist das eine gute Ergänzung dazu, leider nur ein bisschen falsch rum. Wir haben die NINA-App, das

Cellbroadcasting nicht. Das sollte man also dringend beheben. Und zweite Anmerkung: Sie ist nicht Open Source und damit eben auch nur teilweise ideal. Auch da ist man wohl dran, das begrüße ich explizit, wenn man das vornehmen würde. Und insofern ist es also eine wundervolle Ergänzung dieser Warnfunktionalitäten, aber sie ist nun mal nicht das Herzstück. Das Herzstück müsste eigentlich ein Cellbroadcasting sein. Das aus der Sicht NINA-App. Was die LÜKEX-Übungen angeht, die sind sehr wichtig und die sind auch sehr gut. Aber wichtiger ist, daraus resultierendes Feedback umzusetzen. Das haben wir bei der Pandemieübung gesehen, ja? Das ist wirklich ein Drehbuch für das, was wir gerade in der Pandemie erleben. Es wurde quasi eine sehr, sehr vergleichbare Ausbreitung eines Virus geübt. Es wurde jede Menge Feedback zusammengetragen. Das ist übergeben worden an die Verantwortlichen, aber das Feedback ist liegengeblieben. Und das hat so eine extreme Ähnlichkeit zu diesem IT-Sicherheitsgesetz 1.0 – fehlende Evaluierung, aber wir machen schon mal einen Teil 2 und schauen dann mal, ohne dieses Feedback einfließen zu lassen, evaluiert und strukturiert, wie man das optimieren könnte. Zu der Evaluierung gab es ja noch die Anmerkung. Habe ich ja im Endeffekt jetzt schon gesagt: Ich kenne nirgendwo die Situation, dass man eine Evaluierung der Ergebnisse nicht nutzt als Basis für eine Verbesserung. Auch im § 8a BSI-Gesetz für Kritische Infrastrukturen steht ja drin, dass man einen angemessenen branchenspezifischen Stand der Technik umsetzt. Das bedeutet aus der Erwartungshaltung des BSI und dem Stand der Technik eben, dass man sagt, man bringt ein Informationssicherheitsmanagementsystem ans Laufen. Das heißt, man hat ein Plan-Do-Check-Act-Zyklus, in dem man sagt, ich plane was, ich setze es um, anschließend gehe ich in eine Evaluierungsphase und agiere dann erneut und bringe das ein. Und diesen Zyklus, der nennt sich sogar Demingkreis, der ist also wissenschaftlich und nach Stand der Technik belegt, das ist die Funktionsweise, wie man Feedback in eine Struktur einbringt. Und ja, es ist gesetzlich für die KRITIS-Betreiber vorgegeben. Ich vermisse es bei LÜKEX-Umsetzung der Übung, ich vermisse es bei einer BBK-Warntag-Übung. Auch da ist lieber auf den BBK rumgestritten worden als zu sagen: Hey, wir haben hier Feedback und bauen das ein und optimieren, folgende Problemlage haben wir. Und so verhält es sich eben auch mit der Evaluierung des IT-Sicherheitsgesetzes 1.0. Wir sollten also die Zeit nutzen, diese seit 2015 – das sind jetzt sechs Jahre, wenn man die Zeit betrachtet – gelebten § 8a und 8b für KRITIS-Betreiber beispielsweise strukturiert zu analysieren, zu validieren, Feedback einzubringen. Das fehlt immer noch. Und das ist auch definitiv ein Defizit, was in der Grundsubstanz der Struktur schlecht ist.

Dann zu den Fragen von Frau Pau. Es ging um die Zurückhaltung von Sicherheitslücken als Gefährdung der Nutzer, wie ich mir ein Schwachstellenmanagement vorstellen würde und was das praktisch heißt. Ja, wie ich mir eins vorstellen würde, was sozusagen alle Faktoren angemessen adressiert, ist, wie ich auch in meinem Eingangsstatement gesagt habe: Ein hohes Maß an IT-Sicherheit kann man nur erreichen, wenn beispielsweise alle Sicherheitsbehörden, und zwar ausnahmslos, das sind BND, BKA, Bundespolizei, Verfassungsschutz, CITIS, Bundeswehr – ist völlig egal – verpflichtet werden, von ihnen gefundene Sicherheitslücken oder erworbene Sicherheitslücken oder Schwachstellen ausnahmslos an zum Beispiel ein unabhängiges BSI zu melden. Solange diese Pflicht nicht bei allen staatlichen Institutionen gegeben ist, brauchen wir auch nicht darüber reden, wer mitmacht und wer nicht mitmacht. Es reicht ja einer, der nicht mitmacht, und dann fehlt es einfach. Insofern ist das eine Lücke im Gesamtkonstrukt. Und eine Lücke reicht aus, um da einzureißen. Gesetzt dem Fall, es gäbe jetzt ein unabhängiges BSI, welches wirklich ausschließlich für die Defensive da ist und sagt: Alles klar, wir bekommen diese Schwachstellen gemeldet, erkennen sie teilweise auch selbst, dann sollte es diese Informationen ausschließlich und unverzüglich dafür nutzen, im Rahmen eines sogenannten Responsible-Disclosure-Verfahrens diese Informationen an den Hersteller zu geben, damit der ein Beheben und Patching dieser Schwachstellen vornimmt, und die Öffentlichkeit nach Abstimmung mit dem Hersteller zu informieren, damit eben die Kunden, und das sind beispielsweise Endnutzer, die Android oder iPhone verwenden beispielsweise oder Windows 10, was so gängig ist, aber auch Kritische-Infrastruktur-Betreiber, die inzwischen durchaus gängigere Komponenten in ihrem Prozessautomatisierungs- und Produktionsumgebung einsetzen, eben dann verstehen, okay, ich habe folgende Komponente,

ich habe ein Problem und ein Defizit. Hier gibt es noch kein Patch oder der wird bald bereitgestellt und ich muss sozusagen eine mitigierende Maßnahme einsetzen, um die ursprüngliche Problematik zu beheben. Das wäre also ein Schwachstellenmanagementprozess, den ich mir vorstellen und auch wünschen würde. Denn das bedeutet, bedingungslos Schwachstellen auszuräumen. Und warum reicht das für alle Bereiche aus? Naja, Sicherheitsbehörden und Nachrichtendienste können ja auch durchaus den Zeitraum ausnutzen, in dem eine öffentlich bekannt gewordene Schwachstelle noch nicht gepatcht ist. Viele der Ziele werden sicherlich nicht sofort alles patchen. Bei Kritischen Infrastrukturen beispielsweise dauert das nun mal in der Regel länger, als durchschnittlich mal eben schnell ein Patch einspielen, weil eben eine Produktionsanlage dadurch einen Störfall haben kann oder weil beispielsweise eine bestimmte Zertifizierung oder Zulassung aus Haftungsgründen nicht gegeben ist. Insofern gibt es also da auch einen Zeitraum, der durchaus auch lange sein kann und nicht nur ein paar Tage oder Wochen, sondern durchaus auch mal Jahre. Und das sollte in Kombination damit, dass man mit dieser gesamten IT-SiG-2.0-Umsetzung sowieso auch nicht Supply-Chain-Angriffe wie bei SolarWinds adressieren kann, auch nicht mit den Kritische-Komponenten-Zertifizierungen, sollten diese beiden Möglichkeiten wirklich reichlich sein, um aus diesem Repertoire zu agieren, um nachrichtendienstliche und sicherheitsbehördliche Wünsche und Bedürfnisse zu stillen.

Dann kommen wir zum BSI als nicht neutral. Eine fachliche Unabhängigkeit war gefragt als zweite Frage und wie sähe meine Alternative aus. Warum ist es nicht neutral? Nun, es nennt sich halt immer neutrale Behörde, aber es untersteht nun mal dem BMI. Das steht halt im § 1 Satz 2 des BSI-Gesetzes so drin. Und es wurde eben auch in der Vergangenheit gegen den eigenen Willen dazu angeordnet, Dinge zu tun, und zwar beispielsweise die Staatstrojanerunterstützung. Das ist öffentlich geworden. Das BSI hat zu Bedenken gegeben, dass das, wenn das öffentlich wird, eben Vertrauensverlust bedeuten kann. Gut, wir haben nun mal eine Demokratie und diese Informationen sind zum Glück auch öffentlich geworden. Und, ja, dieser Vertrauensverlust ist eingetreten, sowohl in der privaten Wirtschaft – den Unmut kann man in den 24 Stellungnahmen definitiv nachlesen – als auch bei den privaten Endverbrauchern, die eben auch sagen: Bin ich jetzt da an der richtigen Stelle oder sind Sie eben Handlanger der Sicherheitsbehörden und Nachrichtendienste? Und all das zusammen stellt eben auch heraus, dass wir da eine grundsätzliche Gretchenfrage haben. Es schlagen da zwei Herzen in der Brust dem BMI, aber beide müssen bedient werden. Am Ende kann das nur wie ein Pendel ausschlagen, das ist kein Spagat, den man machen kann. Man kann sich für einen oder einen anderen entscheiden, und dieses Pendel schlägt dann in die eine oder andere Richtung aus. Und dafür muss man sich klar entscheiden, dafür braucht man eine Strategie. Die vermisse ich hier.

Es gibt in der Vergangenheit – machen wir es mal ganz generisch – die Zurückhaltung von Schwachstellen, das ist auch schon vorgekommen, aber es ist eben noch nicht so ganz öffentlich. Und insofern haben wir die Problemlage Stand heute sowieso schon. Um das Ziel der Unabhängigkeit zu erreichen – es war ja die Frage, wie sieht meine Alternative aus –, kann beispielsweise, und das ist wirklich nur ein Beispiel, es gibt mehrere Optionen und alle Optionen sind nicht systematisch evaluiert worden, das würde ich also empfehlen, das haben wir sozusagen als Vorschlag unter anderem erarbeitet. Aber auch Dr. Sven Herpig von der Stiftung Neue Verantwortung hat letztes Jahr ein Paper veröffentlicht Mitte/Ende letzten Jahres, wo auch verschiedene Varianten und Formen der Neutralität des BSI dargestellt wurden. Ich empfehle also dringend, das auf jeden Fall zu evaluieren und dann umzusetzen, aber konkret könnte es heißen, dass mindestens eine fachliche Unabhängigkeit vom BMI so aussehen kann, dass dieser § 1 Satz 2 BSI-Gesetz vergleichbar dem Statistischen Bundesamt eben die Formulierung enthält: „Das BSI führt seine Aufgaben auf der Grundlage wissenschaftlich-technischer Erkenntnisse nach den Anforderungen des jeweils fachlich zuständigen Ministeriums durch.“ So hätte man sowohl die Grundlage wissenschaftlich-technischer Erkenntnisse integriert als auch die fachlich zuständigen Ministerien, die manchmal ja offenbar hier auch auf der Strecke bleiben oder irgendwelchem Kuhhandel zustimmen, damit diese Gesetze in dieser Form durchgewunken werden oder vorbereitet werden, wie wir sie hier gerade erleben. Danke schön.

Vors. **Andrea Lindholz** (CDU/CSU): So, dann kommen wir als nächstes zu Herrn Dr. Herpig.

SV **Dr. Sven Herpig** (Stiftung Neue Verantwortung e. V., Berlin): Ja, vielen Dank. Ich beantworte zuerst die Frage von Herrn Hartmann. Also, eine Art, wie ein Schwachstellenmanagementmodell aussehen kann, hat Herr Atug ja gerade skizziert. Eine andere Art wäre ein Schwachstellenmanagementmodell einer etwas komplexeren Form. Da liegt natürlich der Teufel im Detail. Wir haben hierzu ein Jahr lang mit einer interdisziplinären, internationalen Arbeitsgruppe gearbeitet. Wir haben ein Modell entwickelt, das man anwenden könnte, wobei ich da ganz klar auch sage, das ist natürlich nicht der Weisheit letzter Schluss. Da muss man noch mal genau reingucken. Als Grundlage dafür aber, wahrscheinlich auch wie von dem Modell, was Herr Atug gerade vorgeschlagen hat, wäre es, dass es ein zumindest fachlich, also wissenschaftlich unabhängiges BSI gibt, was im BSI-G dann auch festgesetzt wird. Nur so kann das BSI seiner Funktion sowohl als glaubwürdiger Ansprechpartner für zum Beispiel die Sicherheitsforscherinnen und Sicherheitsforscher als auch seiner Zusammenarbeit mit den Behörden wahrnehmen. Alle Schwachstellen, und das ist sehr simplifiziert und verkürzt dargestellt, die dem BSI im Rahmen einer solchen Schwachstelle gemeldet werden würden, müssten direkt in einen Responsible-Disclosure-Prozess gegeben werden, egal ob sie von Sicherheitsforscher*innen kommen oder von anderen Behörden. Es gibt vielleicht einen minimalen Prozentsatz, der hier rausfällt. Gucken wir uns zum Beispiel an Software oder Bibliotheken, wo die Maintainer nicht mehr vorhanden sind, wo man vielleicht erst mal gucken muss, wie geht man mit dieser Schwachstelle um? Natürlich kann man öffentlich darüber berichten, dass es diese Schwachstelle gibt und dass sie nicht mehr patchbar ist oder man sucht eben eine Möglichkeit, hier ein Update programmieren zu lassen, vielleicht von Drittparteien, um so dann selbst den Patchprozess voranzutreiben.

In einem Prozess, wo mehrere Behörden zusammenkommen und dann ihre Schwachstellen einbringen, wie gesagt mit Ausnahme des BSI, und darüber zu diskutieren, ob eine Schwachstelle dann, was damit geschehen soll, wie schadhaft sie ist und was man damit weiter macht, sollte auf jeden Fall das BSI am Tisch sitzen. Und das BSI sollte nämlich deswegen am Tisch sitzen, damit man ihm eine Veto-Funktion einräumen kann. Denn die numerische Überlegenheit liegt ganz klar bei den Sicherheitsbehörden, die ein Interesse daran haben, Schwachstellen auch zurückzuhalten. Deswegen müsste ein vertrauenswürdiger Akteur, der die IT-Sicherheit hoch bewertet, wie zum Beispiel das BSI, ein Vetorecht haben. Und jetzt kommt auch der Übergang, und natürlich bräuchten wir hierfür eine rechtliche Grundlage, die offen ist, nicht nur irgendwie ein Errichtungserlass, wie wir es bei ZITiS gesehen haben, sondern etwas, was in der Öffentlichkeit auch verfügbar ist, an dem wir kritisieren können und wo wir gemeinsam das auch verbessern können.

Übergehend zu der Frage von Herrn Höferlin: Natürlich gäbe es noch eine – sage ich mal – Schwachstellenmanagement-Light-Version, indem man einfach in den Gesetzestexten der Sicherheitsbehörden eine reziproke Meldepflicht einführt. Das BSI hat in seinem Gesetz bereits stehen, dass, wenn ihm Informationen zukommen, die fürs BKA oder andere Behörden interessant werden, dass sie diese Informationen den entsprechenden Behörden weitergeben muss. Ähnlich könnte man gestalten, dass alle anderen Sicherheitsbehörden, sie wurden hier gerade schon aufgezählt, in ihrem Errichtungsgesetz, in ihrem Errichtungserlass vielleicht dann auch, drinstehen haben, dass, wenn ihnen Schwachstellen bekannt werden, die – wenn ausgenutzt – für die IT-Sicherheit in Deutschland nachteilig werden, und das ist wahrscheinlich die weit größte Menge der Schwachstellen, dass diese dann eben dem BSI gemeldet werden können, damit das BSI den Responsible-Disclosure-Prozess einleiten kann oder sich um einen Patch entsprechend kümmern kann.

Dann kommen wir zu den verpflichtenden Mindeststandards für die Verfassungsorgane. Ich würde das sogar noch ausweiten, ich weiß, damit mache ich mir keine Freundinnen und Freunde. Wir sollten hier auch die politischen Parteien vielleicht ab einer bestimmten Mitgliederanzahl mitdenken, denn auch Cyberangriffe gegen politische Parteien sind gerade in den letzten Jahren jetzt nicht ungesehen. Wir haben gesehen, dass die politische Störung, die Einflussnahme auf Wahlen mittlerweile en vogue ist und ein Mittel unterschiedlicher Nachrichtendienste. Von daher

sollten wir die politischen Parteien hier auch mitbedenken, um die IT-Sicherheit auch dort zu erhöhen. Eine Idee, und wie gesagt, das alles muss natürlich auf verfassungsrechtlich soliden Füßen stehen, wäre es, dass Mindeststandards zum Beispiel für Verfassungsorgane dann im Einvernehmen mit dem BSI zu treffen sind. Aber ich glaube, hier einfach die Aussage zu machen, dass die Verfassungsorgane bestimmte Mindeststandards übernehmen können, ist schon mal ein guter erster Schritt, aber vielleicht kann man hier noch weiter gehen und eventuell auch die politischen Parteien einbinden.

Als letzter Punkt die Frage zu den Rückmeldepflichten. Es ist bekannt, glaube ich, dass aus der Wirtschaft, egal aus welcher Ecke, man sehr oft hört, dass sich die Unternehmen, vor allem die, die von einem Cybervorfall dann auch betroffen sind, sich wünschen, mehr Informationen vom BSI zurückzubekommen. Das war auch eine Diskussion, wenn ich nicht ganz falsch liege, im Rahmen der KRITIS-Gesetzgebung. Und ich glaube, an dieser Stelle muss man ganz einfach mal sagen, dann muss man die Vertreter*innen von den Wirtschaftsunternehmen, speziell die IT-Abteilung, die IT-Sicherheitsabteilung, zusammensetzen mit Vertreter*innen vom BSI und dort muss ausdiskutiert werden, welche Informationen denn weitergegeben werden bei einem Vorfall, aber auch abseits von Vorfällen. Das ist, glaube ich, nichts, was man von oben aufdoktrinieren kann. Hier müssen sich die Verantwortlichen zusammensetzen. Hier muss man in guter Arbeitsatmosphäre darüber diskutieren: Was brauchen die Unternehmen, was wollen sie und was kann das BSI dann auch geben, damit man hier auch auf einen gemeinsamen Nenner kommt?

Was noch weiterhelfen könnte wäre – und da gibt es kleine, zarte Ansätze, sowohl beim BSI als noch weniger aber beim Verfassungsschutz –, dass entsprechende Berichte geschrieben werden und mehr Informationen eben mit einem größeren Kreis an Unternehmen geteilt werden über Vorfälle, über Mitigationsmethoden usw. Ganz spannend wäre vielleicht auch, dass man mal darüber nachdenkt, das aktuelle Lagebild, oder ich sage mal so die Lagebilder, zu synchronisieren, vielleicht auch in einem Lagebild zusammenzuführen. Aktuell haben wir das BSI, was ein Lagebild hat und rausgibt, das BKA, was ein Lagebild hat und rausgibt zur Gefährdungslage im Cyberraum, und die Bundeswehr, die ein Lagebild hat, aber nicht öffentlich rausgibt. Die Sachen, die rausgegeben werden, erscheinen einmal im Jahr in einem PDF-Dokument und werden auf einer Pressekonferenz vorgestellt. Ich weiß auch nicht, ob das notwendigerweise noch zeitgemäß ist im Jahr 2021. Also ein kürzerer Zyklus, vielleicht andere Formate würden hier auch vielen Wirtschaftsunternehmen dann auch schon helfen, die Gefährdungslage besser einschätzen zu können und bei akuten Gefährdungen dann auch bilaterale, multilaterale Informationspflichten und Informationsweitergabe zwischen dem BSI, zwischen anderen beteiligten Behörden und den Wirtschaftsunternehmen. Vielen Dank.

Vors. **Andrea Lindholz** (CDU/CSU): Herr Neumann bitte.

SV **Linus Neumann** (Chaos Computer Club Berlin): Ja, vielen Dank. Ich versuche, mich kurz zu fassen. Die Fragen waren einmal danach, ob und wie der Staat seiner Schutzverantwortung nachkommt und dann noch mal spezifisch auf die sogenannten Kryptowars. Ich würde jetzt mal so das Bild eines kleinen mittelständischen Unternehmens in den Raum werfen. Das kauft einfach ein bisschen IT und steht dann mit dem Krempel allein da. Und da hat auch noch nie jemand bei geholfen. Und genau da muss eigentlich IT-Sicherheit proaktiv ansetzen, Problemklassen eliminieren durch Prävention, Detektion und Wiederherstellungskapazitäten. IT-Sicherheit besteht nicht darin, nicht gehackt zu werden, sondern auch im Fall eines Hacks darauf adäquat reagieren zu können. Große Unternehmen schaffen das, weil sie es sich leisten können. Die haben dieses Problemfeld in ihrem Organigramm anerkannt und haben die Verantwortlichkeit dafür geschaffen. Der Staat muss dafür sorgen, dass Sicherheit aber weniger kostet und selbstverständlich wird, weil die Kleinunternehmen und die Bürgerinnen und Bürger, die stehen eben mit dem Krempel alleine da. Und um das zu machen, das ist ja etwas, was ich auch beruflich versuche, ich mache meinen Job ja auch nicht als ewiger PanTester und Strategieberater, um nicht auf eine Erhöhung der IT-Sicherheit hinzuwirken, sondern, weil ich mehr IT-Sicherheit irgendwie besser finde. Das ist so eine ästhetische Frage bei mir. So. Wenn Sie das machen wollen, dann brauchen Sie eine Strategie. Und der Herr Herpig hat da ja mal ein

Schaubild gemacht. Ich glaube nicht, dass er das selber erklären kann und ich glaube auch nicht, dass das BMI oder die Bundesregierung das erklären kann. Das ist eine Wandtapete der Interessenkonflikte, der Verantwortungsdiffussion und der ungenutzten Konsolidierungspotenziale. Da ist eine Strategie nicht zu erkennen. Und die brauchen wir. Und diese Strategie braucht konkrete und kompromisslose Maßnahmen zur Erhöhung von IT-Sicherheit. Dafür brauchen wir eine sichere Basis. Die muss regelmäßig auditiert werden und sie muss auch der Dynamik Rechnung tragen, was Herr Artz ja schon sagte. Stattdessen bekommen wir jetzt ein freiwilliges Sicherheitskennzeichen.

Zur Meldepflicht: Wurde auch schon ausgeführt. Schwachstellen kennen kein Gut und kein Böse, aber Böse kennen Schwachstellen. Und deswegen müssen Schwachstellen abgebaut werden. So. Es hilft nicht, die geheim zu halten. Das muss kompromisslos vorangetrieben werden. Und IT-Sicherheit muss gefördert werden, statt sie durch Bürokratie auszubremsen, ja? Ich habe das ja schon gesagt mit den Unternehmen. Die großen Unternehmen können das machen, aber jede Bürokratie, insbesondere, wenn es eine von außen ist, kostet Ressourcen, die besser in eine sichere Basis investiert werden können. Die Unternehmen wollen ja selbst IT-Sicherheit haben. Es ist ja nicht so, als müsste man denen sagen: Ey, Unternehmen, macht mal sicher hier. Die wollen das ja auch, aber die kriegen es nicht! Und große Unternehmen müssen das wie gesagt, um ihrer eigenen Komplexität gerecht zu werden, tun. Ich sehe da keinen Bedarf von Seiten des BSI, da noch bei zu helfen. Das sind die Kleinen, das sind die Hidden Champions, die allein und hilflos auf weiter Flur stehen. Und denen hilft man nur, wenn man eine sichere Basis schafft. So. Wie schafft man eine sichere Basis? Zum Beispiel ein Pool von auditierter Open Source Software angehen, Bereitstellung von Ressourcen, eine Organisation dafür, dass das gefördert wird und dann eben eine unbürokratische und dauerhafte Förderung von Entwicklungsprojekten. Es gibt viele Sicherheitstools, Sicherheitsansätze, die jedes Unternehmen sehr gut gebrauchen kann. Gleichzeitig, um der Dynamik der IT-Sicherheit Rechnung zu tragen, muss man selber prüfen können. Das ist eingangs schon gesagt, den § 202 zu streichen. Angriffsprogramme soll man nicht nur mit einem rechtlichen Restrisiko benutzen können, sondern man sollte die Anwendung auch tatsächlich ermutigen. Das BSI sollte also stark und unabhängig aufgestellt werden, kompromisslose Meldepflichten für alle staatlichen Stellen, denn IT-Sicherheit ist immer besser als Unsicherheit, weil beides immer für alle gilt. Und deswegen ist auch IT-Sicherheit das einzige übergeordnete Sicherheitsinteresse, von dem überhaupt die Rede sein kann.

Kurzer Bezug zu den Cryptowars. Hier hat sich ja dieser Ausspruch „Sicherheit durch Verschlüsselung und Sicherheit trotz Verschlüsselung“ manifestiert, der genau die Janusköpfigkeit der inneren Sicherheit hier zeigt. Wurde jetzt auch international übersetzt. Auf EU-Ebene werden ja entsprechende Angriffe auf verschlüsselte Kommunikation auch geführt. Ich war vor Jahren hier in Ausschüssen als Sachverständiger zu E-Government-Gesetz und E-Justice-Gesetz. Da haben wir über die De-Mail diskutiert. Da habe ich das damals gesagt: Bitte schafft ein kompromissloses System. Inzwischen stimmt mir Tim Höttges zu, der Vorstandsvorsitzende der Deutschen Telekom, der De-Mail als „toten Gaul“ bezeichnet. Ein System, das kein Mensch jemals nutzt. Messenger, diese verschlüsselten Messenger, auf die jetzt alle eindreschen, das ist die erste unkomplizierte Kryptolösung, die KMU und Gesellschaft zur Verfügung stehen. Das ist Sicherheit durch Verschlüsselung. Punkt! Ohne Trotz. Der einzige Trotz kommt jetzt vom BMI, die alles versuchen, dagegen zu tun. Wer in Deutschland ein sicheres E-Mail-System anbietet, wird am Ende vor Gericht dafür verurteilt und muss es aktiv schwächen, um den Ansprüchen der Strafverfolgungsbehörden gerecht zu werden. Kein Wunder, dass hier keine IT-Sicherheit entsteht. Ich will hier ein kleines Beispiel nennen aus den vergangenen Jahren, aus den vergangenen Monaten: Bei der Corona-Warn-App hatte die deutsche Bundesregierung einmal keine Zeit, zu viele Kompromisse zu machen und musste ein kompromisslos sicheres System bauen. Und statt sich jetzt einmal zu freuen und diesen Erfolg zu feiern, soll jetzt noch der Datenschutz daran schuld sein, dass die Impflogistik versemmelt wird und wir in halbherzigen Lockdowns hängen. Wer so über Probleme nachdenkt und immer nur eine weitere Schuldige sucht, auf die man irgendwie das eigene Versagen abstempeln kann, da wird einfach nichts entstehen. Und daher habe ich tatsächlich – das ist die Antwort auf die

Frage – ich habe den Eindruck, Sie wollen es einfach nicht. Vielen Dank.

Vors. **Andrea Lindholz** (CDU/CSU): Und Herr Schallbruch bitte noch.

SV **Martin Schallbruch** (Digital Society Institute der ESMT Berlin): Ja, vielen Dank. Ich würde gern die Fragen des Abgeordneten Bernstiel in umgekehrter Reihenfolge beantworten. Zunächst zum Thema Schwachstellen: Da ist ja jetzt viel zu gesagt worden. Und ich bin immer ein bisschen irritiert über diese Diskussion, die so ein bisschen so klingt, als würden wir im luftleeren Raum handeln. Wir haben eben nur Aussagen zu Regelungen in dem Gesetzentwurf, der auf dem Tisch liegt, gehört. Darüber ist ein bisschen in Vergessenheit geraten, dass wir im BSI-Gesetz schon heute für alle Bundesbehörden die Verpflichtung haben, Schwachstellen an das BSI zu melden in § 4. Das ist geltendes Recht. Und das BSI hat auch nach dem geltenden Recht die Verpflichtung nach § 8b Absatz 2 Nr. 4 des Gesetzes, beispielsweise die Betreiber Kritischer Infrastrukturen und verschiedene andere darüber zu informieren. Das BSI hat keine Doppelrolle im geltenden Gesetz. Und durch die neuen Regelungen, die in dem BSI-Gesetz in dem vorliegenden Entwurf ergänzt werden, wird nach meinem Eindruck auch keine solche Doppelrolle geschaffen. Vielmehr ist es so, dass in den § 7a und 7b des Entwurfs für das BSI neue Befugnisse eingeräumt werden und diese Befugnisse ausdrücklich nur beschränkt werden auf die Wahrnehmung bestimmter Aufgaben des BSI, und nicht auf die Unterstützung der Polizeien und Strafverfolgungsbehörden und Nachrichtendienste, obwohl dies grundsätzlich auch eine Aufgabe des BSI im Aufgabenkatalog ist. Das heißt, die Bundesregierung hat mit ihrem Entwurf sozusagen eine Art Einstieg in eine Beschränkung auch der Aufgaben des BSI an dieser Stelle vorgenommen. Und das ist nach meinem Eindruck auch in der Tradition des bisherigen Verhaltens des BSI. Ich kenne keine Fälle, in denen das BSI anders gehandelt hat. Und das Beispiel, was eben genannt wurde, dass das BSI den ‚Staatstrojaner' unterstützt hat, ist nicht ganz vollständig dargelegt worden. Das BSI hat nach den Informationen, die veröffentlicht worden sind, allein das IT-Sicherheitskonzept geprüft. Und da wäre ich jetzt ehrlich gesagt beunruhigt, wenn bei einer so sensiblen Informationstechnik wie der Software, die die Nachrichtendienste und Polizeibehörden nutzen, um Quellen-TKÜ-Maßnahmen oder Online-Durchsuchungen durchzuführen, das BSI das IT-Sicherheitskonzept nicht prüfen würde. Es wäre sozusagen ein Desaster. Insofern hat das BSI, ohne dass es dort zu einer irgendwie gearteten Doppelrolle kam, an der Stelle seine Aufgabe wahrgenommen. Natürlich sind die Regelungen, die vorgeschlagenen werden für die §§ 7a und 7b nur ein erster Schritt in einen etwas umfassenderen Prozess, wie wir ihn aus anderen Ländern kennen. Da verschiedene Behörden auch im Verantwortungsbereich des Bundes, zunehmend aber auch im Verantwortungsbereich der Länder nun die Notwendigkeit durch ihre gesetzlichen Regelungen haben, Software einzusetzen, die mit Schwachstellen hantiert, glaube ich, dass wir einen Prozess brauchen, der ein Abwägungsverfahren transparenter macht. Das wird man im laufenden Gesetzgebungsverfahren nicht mehr schaffen können, aber das haben andere Länder auch angefangen und ich glaube, das sollte Deutschland auch tun.

Zweitens die Frage der Unabhängigkeit des BSI. Das BSI ist keine wissenschaftliche Forschungseinrichtung, die Risiken der IT-Sicherheit mit dem Zwecke wissenschaftlicher Publikationen oder öffentlicher Informationen erforscht. Das BSI ist eine operative Bundesbehörde, eine Bundesoberbehörde mit sehr weitreichenden Durchgriffsbefugnissen. Es ist Regulierungsbehörde für Kritische Infrastrukturen, für den Schutz der Bundesverwaltung und der Netze der Bundesregierung verantwortlich. Das BSI ist verantwortlich für die Zertifizierung von IT-Sicherheitsprodukten, für technische Standards, mittlerweile auch für den Verbraucherschutz. Das BSI ist eine sehr weitreichend verantwortliche Bundesoberbehörde. Eine solche Bundesoberbehörde kann und sollte nicht unabhängig sein! Das sage ich jetzt gerade in diesen Kreisen als Botschaft an das Parlament: Eine solche Bundesoberbehörde in die Unabhängigkeit zu schicken, heißt, sie der politischen Verantwortung und auch der Verantwortung gegenüber dem Parlament zu entziehen. Das sieht unsere Verfassung eigentlich nicht vor. Das Grundgesetz geht davon aus, dass wir eine einheitliche Bundesverwaltung haben, dass wir nur in eng begrenzten Bereichen ministerialfreie Räume haben. Und warum sollten wir für ein so wichtiges Politikfeld wie die IT-Sicherheit nun sagen, wir gliedern dieses gesamte Politikfeld aus der politischen

Verantwortung aus? Das wäre ein Fehler, der ähnlich groß wäre, wie wenn man sagen würde: Wir machen jetzt das Luftfahrtbundesamt unabhängig vom Verkehrsminister, weil die könnten ja bei der Untersuchung von Flugzeugen irgendwelche Fehler machen oder irgendwelche anderen Interessen haben. Oder denken Sie sich, das Robert-Koch-Institut – in aller Munde im Augenblick – entziehen wir der Fachaufsicht des Gesundheitsministers. Und wenn die Politik zum Ergebnis kommt, wir brauchen eine neue Teststrategie im Bereich von Corona-Virus, dann sagt das Robert-Koch-Institut: Oh, wir haben gerade anderes vor, wir wollen das nicht machen. Sie Abgeordnete könnten dann den Gesundheitsminister dafür nicht mehr in die Verantwortung nehmen. Das ist die Folge einer unabhängigen Bundesoberbehörde, die wie gesagt die Verfassung eigentlich nicht vorsieht. Deshalb plädiere ich dafür, dass man die möglichen Interessenkonflikte, die es immer gibt bei der Wahrnehmung von Aufgaben innerhalb von Bundesbehörden, zwischen Bundesbehörden oder auch innerhalb der Ministerialverwaltung ebenso austrägt, wie wir es vorgesehen haben. Es gibt dafür gesetzliche Regelungen und es gibt Abstimmungsprozesse, in denen dann am Ende eine politische Entscheidung gefällt werden kann und diese Entscheidung auch politisch durch Sie, durch das Parlament kontrolliert werden kann.

Es wurde eben die Vielfalt der Behörden im Cyberbereich in Deutschland benannt. Und da wird immer darauf verwiesen, wie viele Behörden das sind. Ich bin immer ein bisschen irritiert von der Diskussion, weil die Tatsache, dass sich auch die Staatsanwaltschaften oder die Polizeien nun mit Cybersicherheit beschäftigen, eigentlich eher zu begrüßen ist. Die Tatsache, dass das BSI eine unbestritten national und international unbestrittene Kernstellung als Kompetenzbehörde hat, die viele andere unterstützt und berät, ist glaube ich eher ein positiver Zug unserer Cybersicherheitsarchitektur. Gerade, wenn ich es mit anderen Staaten vergleiche, in denen es eine solche zentrale fachliche Behörde nicht gibt. Das sollte man nicht diskreditieren, nur weil es viele Behörden gibt. Ich lade sie gern mal ein, malen Sie sich zum Beispiel die Verantwortung der Umweltbehörden auch nur eines Landes in Deutschland auf, Sie werden zu einem Bild höherer Komplexität kommen als wir es bei der Cybersicherheit haben, und die Cybersicherheit ist, glaube ich, ähnlich wichtig. Insofern halte ich die Grundstruktur für geeignet und würde sehr davor warnen, dass man den wichtigen Bereich der IT-Sicherheit aus der politischen Verantwortung wegnimmt. Vielen Dank.

Vors. **Andrea Lindholz** (CDU/CSU): Vielen Dank, Herr Schallbruch. Dann kämen wir zur zweiten Fragerunde. Ich hätte ebenfalls zwei Fragen. Eine Frage richtet sich an Herrn Professor Gärditz. In aller Kürze zu dem, was auch gerade Herr Schallbruch ausgeführt hat, dem Thema Unabhängigkeit des BSI. Es ist immer wieder und schon länger in der Debatte. Wie ist Ihre Einschätzung dazu, Herr Professor Gärditz?

Und an Herrn Neumann eine kurze Frage: Sie haben mehr oder weniger gesagt, die kleinen Unternehmen werden weniger dabei unterstützt, sich sicher aufzustellen. Wir haben ja auch in den Ländern schon unglaublich viel auch zu dem Thema gemacht. Mich würde interessieren, wie Sie das bewerten, was von den Landesämtern hier schon geleistet wird, und wo Sie wirklich sagen, da steht ein kleines Unternehmen heute ganz alleine da. Ich habe schon den Eindruck, dass die Situation da besser geworden ist. Ich will jetzt nicht sagen, dass man es nicht noch verbessern kann. Aber mich würde das wirklich mal ganz konkret interessieren, weil es auch immer wieder ein Thema von Kleinunternehmern ist. Ich hatte den Eindruck, so ganz blank wären wir da nicht mehr. Und ob es wirklich so zielführend ist, wenn alles beim Bund angesiedelt ist? Also, ich denke auch, so eine gewisse Verteilung im föderalen System, auch anknüpfend an das was Herr Schallbruch sagte, könnte vielleicht an der Stelle auch nützlich sein. Aber vielleicht können Sie zu den kleinen Unternehmen einfach noch mal was sagen.

Die Union hatte sich noch gemeldet mit Herrn Amthor. Bitte.

Abg. **Philipp Amthor** (CDU/CSU): Frau Vorsitzende, liebe Kolleginnen und Kollegen, das Gute ist, dass man auch in der Regierung unterscheiden kann zwischen Verbesserungsvorschlägen und vernichtender Kritik. Wir haben es hier überwiegend – das will ich noch mal sagen – mit sinnvollen Regelungen zu tun, aber Verbesserungsvorschläge würde ich in der Tat gerne noch mal aufnehmen, auch konstruktiv zu dem neuen B-BSI-Gesetz, zu der Untersagungsnorm. Deshalb zwei

Fragen an Herrn Professor Gärditz. Eine bezüglich des Verfahrens und eine bezüglich der materiellen Regelung. Wenn wir uns den Verfahrensgang anschauen, haben Sie gesagt, der Verfahrensablauf innerhalb der Bundesregierung ist so ohne Beispiel, also dass ein Ressort sozusagen blockieren kann. Und die Norm würde dann auch durch die Beweisschwierigkeiten kaum angewendet werden. Könnten Sie da noch mal einen Vorschlag machen, was könnte man konkret machen sozusagen an der Verfahrensnorm, dass die Untersagung potenziell zur Anwendung kommen könnte? Insbesondere vielleicht der Blick darauf: Ergibt es nicht Sinn, nicht auf unwahre Tatsachen – im Übrigen sprachlich spannend, unwahre Tatsachen gibt es natürlich nicht, sondern unwahre Tatsachenbehauptungen –, wenn man darauf abstellen würde, dass es solche vielleicht gar nicht gibt oder wenn man sagt, mit hoher Wahrscheinlichkeit operierend. Also, was müsste man am Verfahren ändern, damit die Untersagungsnorm greift?

Und zweitens zum materiellen Kern. All die Fragen, die hier vorgeschlagen wurden, ob die Bundesregierung jetzt per Kabinettsbeschluss, per Bundessicherheitsrat entscheidet, was auch immer, das betrifft natürlich auf dem Hintergrund der Wesentlichkeitstheorie nicht die Verantwortung des Parlaments, sondern die Abläufe innerhalb der Regierung machen ja die Wahrnehmung der Regelungsverantwortung beim Parlament nicht mehr oder weniger wesentlich, sondern die Frage wäre: Was müssten wir denn hier eigentlich noch leisten? Müssten wir – das ist sozusagen der zweite Teil – materiell dann Kriterien positiv definieren oder müsste man ggf. das, was in der Allgemeinverfügung per Verwaltungsakt vorgesehen ist, müsste man das per parlamentsgesetzlicher Regelung zumindest in den Grundlagen machen oder per Verordnungsermächtigung oder was auch immer? Würde das helfen, der Verfassungswidrigkeit auf dem Hintergrund der Wesentlichkeitstheorie Abhilfe zu schaffen? Vielen Dank.

Vors. **Andrea Lindholz** (CDU/CSU): Frau Cotar.

BE Abg. **Joana Cotar** (AfD): Ja, vielen Dank. Ich habe noch zwei Fragen an Herrn Artz. In Ihrer Stellungnahme beklagen Sie eine multidimensionale Regulierungsgemengelage, die sich aus der Vielzahl der relevanten Gesetzestexte ergibt und die zu einer Komplexität führt, die für die IT-Sicherheit grundsätzlich abträglich ist. Sehen Sie Stellen im IT-Sicherheitsgesetz, die im offenen Widerspruch zu anderen Gesetzestexten sind und hat Bitkom Vorschläge, wie die regulatorische Komplexität insgesamt verringert werden könnte? Und Sie bemängeln auch, dass eine eindeutige Definition konkreter Schutzziele im IT-Sicherheitsgesetz 2.0 fehlt. Können Sie sich erklären, warum die Bundesregierung auf die Definition von diesen Schutzzielen verzichtet hat? Und gibt es bereits Quellen, an denen sich die Bundesregierung hätte orientieren können, also zum Beispiel andere Gesetze, Industriestandards oder Verbandsstellungnahmen? Danke.

Vors. **Andrea Lindholz** (CDU/CSU): So, dann kommen wir jetzt zu Herrn Hartmann bitte.

BE Abg. **Sebastian Hartmann** (SPD): Liebe Frau Vorsitzende, ich habe zwei Fragen, Ihre Option Drei ziehend, an zwei Sachverständige. Die erste Frage geht an Herrn Artz: Sie haben in Ihrer Stellungnahme die Wechselwirkung des IT-Sicherheitsgesetzes mit anderen Gesetzen, insbesondere dem TK-Modernisierungsgesetz beschrieben. Das ist ja ein zweites Werk, das gerade in der Mache ist. Und ich glaube, dass es vielleicht doch mal hier sinnvoll ist, das zu veranschaulichen anhand von konkreten Beispielen. Etwas fremd in dem Gesetzestext erscheint der § 10 Absatz 6 zur Standardsetzung in der Frage der Open-RAN-Technologie. Warum findet sich so etwas eigentlich im IT-Sicherheitsgesetz 2.0 und nicht irgendwo, wo man es eher vermuten würde – beim TK-Modernisierungsgesetz in der entsprechenden Novelle? Vor allen Dingen, wo Sie gerade auch ja auch über die Standardisierung und die Normensetzung gesprochen haben unter Berücksichtigung internationaler Standards. Das wäre meine Bitte, das am konkreten Beispiel mal darzulegen und Ihre Empfehlung dazu hören.

Und der zweite Punkt, auch wieder technikbezogen und ganz aktuell in der Diskussion, an Herrn Dr. Herpig: Sie haben in Ihrer Stellungnahme ausgeführt und auch an anderer Stelle, dass es eine zunehmende Bedeutung der softwaredefinierten Seite von kritischen Komponenten und entsprechenden IT-Produkten gibt. Könnten Sie das am Beispiel der 5G-Netze mal deutlich machen, wie Sie sich eine Regulierung vorstellen würden? Wir haben viel über Vertrauenswürdigkeit gesprochen, über die Frage von Zertifizierung, auch der politisch-strategischen Entscheidung, die

dahintersteht. Der Kollege Amthor ist noch mal auf die Verfassungswidrigkeit aus Sicht der Union des § 9b eingegangen, was man da tun muss. Vielleicht könnten Sie die technische Seite noch mal darlegen, wie Sie das Zusammenspiel zwischen Software und Hardware sehen und was man vielleicht an genauerer Definition von kritischen Komponenten vornehmen müsste, damit dieses Gesetz tatsächlich anwendbar ist und auch zu einer Erhöhung der IT-Sicherheit in Deutschland führen würde. Herzlichen Dank.

Vors. **Andrea Lindholz** (CDU/CSU): Herr Hartmann, vielen Dank. Dann Herr Höferlin.

BE Abg. **Manuel Höferlin** (FDP): Danke schön, Frau Vorsitzende. Ich schließe an die Frage an. Und die erste Frage geht an Herrn Herpig: Und zwar schreiben Sie in Ihrer Stellungnahme, der Referentenentwurf betrachtet die notwendige Reform der offensichtlich dysfunktionalen zentralen Akteure der deutschen Cybersicherheitsarchitektur, dem Nationalen Cyberabwehrzentrum und dem Cyber-Sicherheitsrat nicht. Deswegen meine Frage: Welche Weichenstellungen für eine Cybersicherheitsarchitektur in Deutschland, die dann bei Sicherheitsvorfällen vor Ort auch schnell helfen kann und gleichzeitig die Bedrohungslage im Ganzen im Blick hält, sollte denn Ihrer Meinung nach im IT-Sicherheitsgesetz getroffen werden? Vielleicht können Sie dazu was ausführen?

Und die zweite Frage würde ich gern an Martin Schallbruch richten: Herr Schallbruch, Sie schreiben in Ihrer Stellungnahme, dass die EU-Kommission ja im Dezember letzten Jahres den Entwurf einer neuen NIS-Richtlinie vorgelegt hat und dass es zwangsläufig eigentlich zu einem IT-Sicherheitsgesetz 3.0 kommen muss und dass es dazu führt. Vielleicht können Sie mal einen Blick in die nahe Zukunft werfen: Welche Punkte müssten denn im IT-Sicherheitsgesetz 3.0 adressiert werden, damit die Wirtschaft besser geschützt wird, dass exponierte Stellen des Bundes besser beschützt werden und dass die Cybersicherheit in Deutschland insgesamt besser geschützt wird? Weil ich befürchte ja, das IT-Sicherheitsgesetz 2.0 wird diese Legislatur durchkommen, egal wie.

Vors. **Andrea Lindholz** (CDU/CSU): Frau Domscheit-Berg bitte.

Abg. **Anke Domscheit-Berg** (DIE LINKE.): Vielen Dank, Frau Vorsitzende. Ich hätte zwei Fragen an Manuel Atug, die ich gerne stellen möchte. Zum ersten interessiert mich einiges rund um das IT-Sicherheitskennzeichen. Es gab ja vom BSI selber zum Safer Internet Day eine repräsentative Umfrage. Da haben 70 Prozent der Befragten gesagt, sie wünschen sich mehr Hilfestellung im Bereich IT-Sicherheit. Es gibt ja auch immer mehr elektronische Geräte im Alltag, von den bekannten smarten Toastern bis zur Waschmaschine. Es braucht also definitiv mehr Verbraucherschutz. Deswegen wüsste ich von Herrn Atug gern, wie er denn vor diesem Hintergrund das freiwillige Sicherheitskennzeichen bewertet, also was die Folge einer solchen Freiwilligkeit eigentlich in der Praxis wäre und auch was er davon hält, dass die Vergabe des Sicherheitskennzeichens im Regelfall ja so ist, dass Hersteller irgendwelche Akten mit Behauptungen zur IT-Sicherheit einreichen und das BSI anhand dieser Aktenlage die Plausibilität prüft. Das wüsste ich gern, ob er das für eine geeignete Grundlage hält, um Konformität mit IT-Sicherheitskennzeichen festzustellen.

Ich kann mich erinnern, dass ich mit Herrn Atug vor kurzem bei der BSI IT-Sicherheitskonferenz war und das BSI mit mehreren Forscher*innen genau dieses Thema hatte. Eine dieser Forscherinnen kam nämlich vom BSI und hat Sicherheitslücken in medizinischen Geräten untersucht. Und ich fragte sie, ob sie irgendeine dieser Lücken, die sie da gefunden hatte – das waren sehr viele – auch auf Basis der Papierlage gefunden hätte. Also zumindest in diesem Fall hat sie das verneint. Ich wüsste dazu auch gern, ob Herr Atug glaubt, dass so ein Kennzeichen, das auf QR-Codes basieren soll, den Durchschnittsverbraucher*innen verlässliche und einfach zugängliche Informationen liefert.

Und in einer zweiten Frage das Thema Evaluierung. Einiges ist da schon beantwortet. Ich wüsste gern, ob das Argument der Bundesregierung überzeugt, dass das für ein Gesetz, das künftig nicht mehr gelten soll, weil es durch ein anderes ersetzt wird, gar keinen Sinn mehr machen würde, da eine Evaluierung zu machen, denn rückwirkend sei das ja nicht sinnvoll oder ob er der Meinung ist, dass auch rückwirkende Evaluationen etwas bringen. Danke.

Vors. **Andrea Lindholz** (CDU/CSU): Und dann haben wir noch Frau Rößner.

Abg. **Tabea Rößner** (BÜNDNIS 90/DIE GRÜNEN): Ja, vielen Dank, Frau Vorsitzende. Ich habe zwei Fragen. Die erste richtet sich an Manuel Atug, und zwar noch mal den Bereich Kritische Infrastrukturen. Ich habe ja beim ersten IT-Sicherheitsgesetz nicht verstanden, wie die Grenzziehungen oder Definitionen sind. Also ein Krankenhaus – bitte korrigieren Sie mich, falls ich da falsch liege – mit einem Einzugsbereich von 500.000 Patient*innen fiel unter das IT-Sicherheitsgesetz 1.0. Als Patientin einer Privatklinik, die irgendwo an der Peripherie ist, möchte ich aber natürlich genauso wenig Opfer eines IT-Angriffs werden, wenn ich zum Beispiel am offenen Herzen operiert werde. Sie verstehen wahrscheinlich, worauf ich hinaus will. Hat sich daran jetzt an dieser Grenzziehung was verbessert? Wie beurteilen Sie das? Was sind denn Ihrer Meinung nach Unternehmen mit besonderem öffentlichem Interesse und warum fallen derzeit – so die Antwort der Bundesregierung auf eine Frage eines Kollegen – die Hersteller von COVID-19-Impfstoffen unter diese Definition? Vielleicht haben Sie eine Erklärung dafür.

Und die zweite Frage geht an Sven Herpig: Das Schaubild hatte Linus Neumann ja eben schon angesprochen, wo es um die verschiedenen Stellen innerhalb der Bundesregierung geht, die mit IT-Sicherheitsthemen beschäftigt sind. Haben Sie den Eindruck, dass es klare Zuständigkeiten gibt und so etwas wie eine kohärente IT-Sicherheitspolitik innerhalb der Bundesregierung?

Vors. **Andrea Lindholz** (CDU/CSU): Frau Rößner, vielen Dank. Wir haben später angefangen, insofern hoffe ich, dass es in Ordnung ist, wenn wir um ein paar Minuten überziehen. Ich habe nur an die Sachverständigen die Bitte, so präzise wie möglich zu antworten, damit wir nicht allzu sehr nach hinten rauskommen. Wir fangen im Alphabet jetzt umgekehrt an und beginnen insofern mit Herrn Schallbruch bitte.

SV **Martin Schallbruch** (Digital Society Institute des ESMT Berlin): Ja, vielen Dank. Manuel Höferlin hatte gefragt nach den Auswirkungen, die die Veränderung der NIS-Richtlinie der EU haben wird. Die EU-Kommission hat am 16. Dezember einen Entwurf einer Neufassung dieser Richtlinie vorgelegt. Diese Richtlinie muss dann in Deutschland nach Verabschiedung in Brüssel binnen 18 Monaten in deutsches Recht umgesetzt werden. Wann sie verabschiedet wird, kann ich Ihnen zum gegenwärtigen Zeitpunkt noch nicht sagen. Die Richtlinie ist ebenso wie das IT-Sicherheitsgesetz 2.0 im Grunde eine Weiterentwicklung des gleichen Themenbereichs, weil das IT-Sicherheitsgesetz 1.0 und die nachfolgende Gesetzgebung ohnehin auf der NIS-Richtlinie der EU basiert, damit wir europaweit eine einheitliche IT-Sicherheitsrechtslage auf diesem Feld haben. Insofern wird dort über das gleiche diskutiert wie hier gerade vor Ort. Es gibt einige Gemeinsamkeiten, beispielsweise die Erweiterung des IT-Sicherheitsrechts und der Regulierung auf weitere Bereiche der Wirtschaft über Kritische Infrastrukturen hinaus. Das hatte ich in meinem Eingangsstatement erwähnt, dass die EU-Kommission hier einen anderen Ansatz wählt und eine branchenbezogene Erweiterung vorsieht. Also für bestimmte Produktionsbereiche, für bestimmte Dienstleistungsbereiche und ansonsten das System der Kritischen Infrastruktur im Großen und Ganzen überträgt. Es gibt dann allerdings eine ganze Reihe von etwas veränderten Regulierungsprinzipien, welche die nationalen Regierungen in ihrer Umsetzung vorsehen müssen. Was die Kontrolle der IT-Sicherheit bei den Unternehmen angeht, unterscheidet sich das teilweise signifikant von dem, was wir hier in Deutschland im IT-Sicherheitsgesetz 2.0 haben. Es gibt einige spezielle Regelungen für beispielsweise Domain Name Service-Provider, die man in Deutschland einführen müsste. Und es gibt einige Regelungen, die beispielsweise die Informationszusammenarbeit betreffen zwischen den Unternehmen und auch mit dem Staat, die wir in dieser Form auch nicht haben. Dort schlägt die EU-Kommission neue Instrumente für Information Sharing vor. Auch die öffentliche Verwaltung – von Herr Höferlin angesprochen – soll nach dem Richtlinienentwurf unter die weiteren Bereiche fallen. Da muss man sehen, ob das dann in Brüssel tatsächlich so bleibt, weil würde die EU möglicherweise ihre Kompetenz überschreiten, wenn sie die öffentliche Verwaltung umfassend regeln würde. Insofern ist klar, dass, egal wie jetzt die Abstimmung in Brüssel und das Gesetzgebungsverfahren von Rat und Parlament aussieht, das IT-Sicherheitsgesetz in der nächsten Wahlperiode noch einmal überarbeitet werden muss, um die

Veränderung der NIS-2-Richtlinie aufzunehmen.

Vors. **Andrea Lindholz** (CDU/CSU): Herr Schallbruch, vielen herzlichen Dank. Jetzt kommt Herr Neumann.

SV **Linus Neumann** (Chaos Computer Club Berlin): Ja, vielen Dank. Ihre Frage war spezifisch zur Situation von kleineren Unternehmen im Bereich der IT. Das ist ein Feld mit großer Dynamik und vor allem – wir haben jetzt sehr viel über Schwachstellen gesprochen – die müssen eben beseitigt werden. Das ist im Prinzip also eine Nachsorge an dem Produkt, was bei den Kund*innen sich dann befindet. Und hier in diese Nachsorge nicht zu investieren, bietet eigentlich einen Marktvorteil. Man kann das Produkt günstiger anbieten, weil man quasi diese Ewigkeitskosten nicht hat. Und ich denke, dass wir diesen Marktvorteil eliminieren müssen. Einerseits durch Haftung, ganz klar, Haftung für Fahrlässigkeit und mangelnde Nachsorge an derartigen Produkten, die sich dann zum Sicherheitsrisiko für ihre Nutzer*innen und für die Bundesrepublik Deutschland entwickeln können. Und mir ist auch nicht ganz klar, wieso überhaupt IT-Produkte mit so großzügigen Haftungsfreistellungen verkauft werden können. Es ist mir eigentlich unklar, weil ich kein Produkt kenne, was so frei von jeder Haftung gehandelt werden kann, außer vielleicht illegalisierte Substanzen. Wir denken insofern an ein Mindesthaltbarkeitsdatum, das also die Hersteller*innen dazu zwingt, Produktmängel im Feld abzustellen. Das ist der Vorteil von IT-Produkten, auch von IoT-Produkten. Ich kann das als unfertiges Produkt ausliefern, ich kann diese Nachsorge vornehmen, also sollten doch bitte auch die Hersteller*innen verpflichtet sein, das zu tun. Warum sollten sie verpflichtet sein? Denn nur, wenn diese Anforderungen für alle gelten, ist es kein Marktvorteil mehr, gegen sie zu verstoßen, und das geht eben nicht anders als durch Zwang und das eben zu einer Markteintrittsvoraussetzung zu machen. Mit IoT geht das Drama einfach nur weiter. Wir haben jetzt auch einfach nur noch viel mehr IT-Systeme in den Netzen hängen. Und es endet natürlich auch nicht, wenn nun leider viele Unternehmen in die Cloud wandern, wo natürlich auch Sicherheitsanforderungen entsprechend geboten wären, sichere Authentifizierung, das Ende der Passwörter zum Beispiel könnte das BSI aktiv vorantreiben. Ich bin mir auch sicher, dass es da Initiativen zu gibt. Demgegenüber ist so ein freiwilliges IT-Sicherheitskennzeichen, das ist total schön, ich bin mir auch sicher, es wird total gut aussehen, aber es wird eben diesen messbaren Effekt nicht haben. Denn die höheren Preise, die jetzt in so ein schön bemaltes Produkt gehen, die muss ich ja immer noch rechtfertigen, und es wird immer noch Menschen geben, die dann eben die Sachen günstiger kaufen. Und die Produkte werden eben nicht nur zum Risiko für sich selber, sondern eben auch zum Risiko für Personen, die sie nicht betreiben, wenn sie jetzt also zum Beispiel in Bot-Netzen zusammengeschlossen sind.

Abschließend will ich noch ganz kurz eine inhaltliche Korrektur zu Herrn Schallbruch machen. Das IT-Sicherheitskonzept des Staatstrojaners hat der CCC geprüft, als wir ihn endlich in den Fingern hatten, und konnten dann eben feststellen, dass er mit den rechtlichen Vorgaben und dem Grundgesetz nicht in Einklang zu bringen war. Und ich denke, genau dieses Beispiel zeigt, dass sich Schadsoftwareentwicklung einfach für ein Bundesamt für Sicherheit in der Informationstechnik nicht ziemt, und das ist genau der zweifelhafte Auftrag, der so viel Vertrauen kostet. Was die Unabhängigkeit angeht war ich jetzt überrascht, weil ich zumindest die Bundesbeauftragte für Datenschutz und Informationsfreiheit als unabhängige und somit eigenständige oberste Bundesbehörde kenne. So ungefähr würde ich mir das für das BSI auch vorstellen. Vielen Dank.

Vors. **Andrea Lindholz** (CDU/CSU): Herr Dr. Herpig.

SV **Dr. Sven Herpig** (Stiftung Neue Verantwortung e. V., Berlin): Ja, vielen Dank. Einmal eine kurze Vorbemerkung zum Kommentar von Herr Schallbruch zu der Weitergabe von Schwachstellen durch andere Sicherheitsbehörden: Wenn § 4 Absatz 3 des BSI-G wirklich so einschlägig ist, dann könnte man ja auch vorschlagen, den Halbsatz am Ende, „soweit andere Vorschriften dem nicht entgegenstehen“, zu streichen, dann hätten wir es hier ganz klar, dass andere Bundesbehörden, auch alle Sicherheitsbehörden, ihre Schwachstellen immer messen und weitergeben müssten.

Dann komme ich jetzt einfach mal zu dem gesammelten Werk der deutschen Cybersicherheitsarchitektur. Unser Wimmelbild, Linus, kann ich dir auch nicht so genau erklären, aber danke, dass du

gefragt hast. Wir haben aber ein 80-seitiges Begleitheft dazu. Und natürlich sind die Zuständigkeiten nicht alle 100 Prozent klar, aber ich glaube, sie sind im Großen und Ganzen zumindest für die handelnden Behörden schon relativ klar. Natürlich könnte man über die ein oder andere Sache noch diskutieren, zum Beispiel, warum die Zurechnung und Zuschreibung von Cyberangriffen nur beim Bundesamt für Verfassungsschutz liegt und nicht vielleicht auch in gleichen Teilen beim Bundesamt für Sicherheit in der Informationstechnik, die hier die hauptsächliche technische Analyse machen, aber im Groben und Ganzen könnte man sagen, dass die Zuständigkeiten so grob hinkommen, aber – und das möchte ich noch zu der Frage weiter hinzufügen – so weit zu gehen zu sagen, dass Deutschland eine kohärente Cybersicherheitspolitik verfolgt, würde ich hier auf keinen Fall.

Die Frage nach der Reform, also was sollte man da tun, damit es kohärenter wird, damit es passender wird? Wie angezeigt, wir haben hier zentrale Stellen wie den Cyber-Sicherheitsrat, wie das Nationale Cyberabwehrzentrum und auch wie das BSI. Leider ist zum Beispiel für das Nationale Cyberabwehrzentrum, was sich scheinbar im dauerhaften Reformmodus befindet, immer noch keine klare, transparente öffentliche rechtliche Grundlage zugänglich. Das wird über Verwaltungsvereinbarungen geregelt. Langsam werden die Länder mit einbezogen, aber da haben wir, glaube ich, noch viel Arbeit vor uns. Der Cyber-Sicherheitsrat, alle Personen, mit denen ich gesprochen habe, können mir immer noch nicht erklären, was genau der Cyber-Sicherheitsrat macht und wirklich beiträgt, um die Strategie in Deutschland voranzutreiben und nicht nur irgendwelche wissenschaftlichen Berichte ab und zu mal zu veröffentlichen. Auch da besteht akuter Handlungsbedarf oder vielleicht sogar Abschaffungsbedarf, wenn er die Strategie in Deutschland nicht vorantreibt.

Zu dem Thema Einbindung der Mobile Incident Response Teams brauchen wir auch hier mehr Klarheit. Das Bundeskriminalamt soll welche bekommen haben, das Bundesamt für Verfassungsschutz und der BND sollen auch ähnliche bekommen haben. Hier ist natürlich bei den nachrichtendienstlichen Incident Response Teams nicht ganz klar, was sie machen. Wir brauchen hier eine Gesamtstrategie, was diese Incident Response Teams machen, wann sie Daten weitergeben, wie sie sich zusammen verknüpfen. Wünschenswert natürlich über ein funktionales, nationales Cyberabwehrzentrum. Vielleicht auch unter Einbindung des Konzepts des Cyberhilfswerks, der AG KRITIS und natürlich ganz klar auch unter Einbindung der entsprechenden föderalen Strukturen, die ja auch sehr nah meistens am Incident direkt dran sind.

Als vorletzter Punkt dazu: Natürlich bedingt das auch ein unabhängiges BSI und nicht, wie gerade gesagt wurde, das Modell Statistisches Bundesamt ist keine fachliche Unabhängigkeit und auch keine vollständige Unabhängigkeit vom BMI, sondern es hat in seinem Gesetz stehen, dass es auf Basis wissenschaftlicher Erkenntnis arbeitet und unterliegt daher der Kontrolle der einschlägigen Ministerien, mit denen es zusammenarbeitet. Und sowas wäre auch ein Modell. Wir haben verschiedene Modelle skizziert.

Als letzter Punkt ganz kurz vielleicht noch zum Thema kritische Komponenten und 5G. Da wurde schon vieles heute gesagt. Von daher werde ich mich da sehr kurz halten. Ich bin nach wie vor der Meinung, dass das IT-Sicherheitsgesetz definitiv und das BSI-G nicht der richtige Ort ist, um dieses Gesetzespaket hier reinzubringen. Es ist klar, dass das statische Vorgehen über Zertifizierung, Aufbau von Zertifizierungsinfrastrukturen, Aufbau von Personal nicht dazu führen wird, dass wir das Thema 5G in den Griff kriegen würden, weil, bis diese Strukturen aufgebaut sind, sind schon Fakten geschaffen. Die Betreiber haben schon die Hardware und die Software entsprechend ausgerollt. Daher brauchen wir da ein nuancierteres, ein dymamisches Verfahren, was es zu entwickeln gilt, aber bitte dann doch außerhalb des IT-Sicherheitsgesetzes und außerhalb des BSI-G. Vielen Dank.

Vors. **Andrea Lindholz** (CDU/CSU): Herr Professor Gärditz bitte.

SV **Prof. Dr. Klaus F. Gärditz** (Rheinische Friedrich-Wilhelms-Universität Bonn): Erste Frage von Ihnen, liebe Frau Vorsitzende – Unabhängigkeit des BSI. Verfassungsrechtlich ist das kaum umsetzbar. Ich darf an das anschließen, was Herr Schallbruch schon gesagt hat. Es gibt eine ständige Rechtsprechung des Verfassungsgerichts, wonach eine Behörde jedenfalls dort, wo sie amtliche Entscheidungen zu treffen hat, und dazu gehören zum Beispiel hier die relevanten Grundrechtsein-

griffe, rückgekoppelt sein muss an die demokratische Willensbildung. Die läuft verfassungsrechtlich so, dass durch Wahlen ein Parlament bestimmt wird, das Parlament – in dem Fall der Bundestag – wählt die Bundeskanzlerin, die eine Regierung einsetzt und Ministerien, und die Ministerinnen und Minister sind verantwortlich für ihren jeweiligen Ressortbereich. Damit geht einher, dass Weisungen erteilt werden müssen, die die Verwaltungen Top-Down steuern, um diese Verantwortlichkeit gegenüber dem Parlament in die Gegenrichtung dann sicherzustellen. Das ist auch eine sehr sinnvolle und notwendige Einrichtung. Unabhängigkeit wird immer so verklärt als besondere Garantie von Neutralität, Sachlichkeit. Das stimmt aber natürlich nicht. Eine unabhängige Einrichtung entwickelt auch ihr Eigenleben. Dann ist aber niemand mehr zur Verantwortung zu ziehen. Sie als Abgeordnete des Deutschen Bundestages müssen eigentlich ein großes Interesse daran haben, dass sie die Regierung für etwaige Fehler, die passieren, auch zur Verantwortung ziehen können. Wenn das BSI unabhängig wäre, das wurde schon gesagt, dann könnte zum Beispiel der BMI nicht mehr parlamentarisch Rede und Antwort stehen, dann müsste man das schicksalsgegeben hinnehmen. Das kann kein sinnvolles Organisationsmodell sein. Wissenschaftliche Tätigkeit einer Behörde bedarf natürlich keiner Weisungen. Nur dann muss ich halt diesen wissenschaftlichen Sektor organisatorisch so abtrennen, dass man den autonom und dann ggf. auch mit Wissenschaftsfreiheit der dort Tätigen organisiert. Das kennen wir für viele Forschungseinrichtungen des Bundes, das RKI wurde schon genannt. Es gibt noch eine ganze Reihe, vielleicht so an die 15 solcher, auch im Forschungsbereich tätigen Bundeseinrichtungen. Das hat aber nichts mit den operativen Befugnissen zu tun, für die wir eine demokratische Verantwortlichkeit verfassungsrechtlich eindeutig brauchen. Der Vergleich zum BfDI hinkt etwas, schon deswegen, weil dort die Unabhängigstellung und die Konstruktion als oberste Bundesbehörde auf eine unionsrechtliche Vorgabe zurückgeht, die das verlangt, nämlich die EU-Datenschutzrichtlinie und insoweit das Unionsrecht gegenüber dem nationalen Verfassungsrecht vorrangig ist. Die Frage, ob das beim BfDI notwendig gewesen wäre, spare ich mir an diesem Ort. Fürs BSI jedenfalls geht das nicht.

Herr Amthor hatte noch zwei Fragen, die genau das aufzeigen, was ich eigentlich möchte. Ich habe meine Stellungnahme auch nicht als Abrissbirne verstanden, sondern als Anregung, konstruktiv nachzubessern, um den Zielen des Gesetzes, die ich ausdrücklich billigen würde, zur besseren Durchsetzung zu verhelfen.

Zur Verfahrensseite – Was könnte man machen, damit das Beweismaß zum Beispiel oder diese Blockade durch die Einstimmigkeit und die Monatsfrist hier aufgehoben würde? Erstens, eine Fristbindung für Entscheidungen müsste ich entweder streichen oder deutlich großzügiger ausgestalten. Etwa im Außenwirtschaftsrecht sind Fristen von drei, respektive vier Monaten etabliert. Das ist dann möglicherweise realistisch, wenn man auf eine Frist im Interesse des beschleunigten Netzausbaus nicht verzichten möchte. Was die Entscheidung angeht, reicht es etwa aus, dass wesentliche Entscheidungen bereits vom Bundeskabinett, wenn sie ressortübergreifende Bedeutung haben, was hier oft der Fall sein wird, zur Kabinettssache gemacht werden. Dann muss eben das Kabinett entscheiden, das entscheidet aber durch Mehrheit und nicht einstimmig. Der derzeitige Entwurf kann dazu führen, dass ein einzelnes Ressort aus willkürlichen Gründen sagt: Nö, ich lege mein Veto ein. Ich will das nicht. Zum Beispiel, weil der Ressortminister Sympathien zu einem hochrangigen Regierungsmitglied eines anderen Staates hat. Solche Männerfreundschaften sollen ja manchmal eine Rolle spielen. Das kann kein sachgerechtes Kriterium sein. Ein Kabinettsbeschluss könnte das überspielen.

Was das Beweismaß angeht, würde ich mich einfach an dem anlehnen, was typischerweise im Recht der Gefahrenabwehr, um das es hier geht, der Standard ist. Dort brauche ich eine gefahrengestützte Prognose. Und ich würde einen Vorschlag in die Richtung machen, dass man sagt: Wenn tatsächliche Anhaltspunkte zum Beispiel den Verdacht begründen, dass eine bestimmte Komponente nicht vertrauenswürdig ist, ja? Oder wenn die gegen die Vertrauenswürdigkeit sprechen. Das wäre ein Verdachtsgrad, der dann eine überwiegende Wahrscheinlichkeit erfordert. Das muss für eine prognosegestützte Gefahrenabwehrperspektive ausreichen. Dann wäre die Norm auch operabel. Es gibt am Ende ja immer noch ein Interventionsermessen, das dem BMI sicherlich

niemand nehmen wird.

Was die inhaltliche Ausgestaltung angeht: Ja, wir brauchen Entscheidungskriterien, die vergesetzlicht werden. In das Gesetz müssen natürlich nicht die technischen Fragen geregelt werden. So etwas lässt sich auch schwer in Gesetzgebung packen. Auch eine Rechtsverordnung ist dafür vielleicht nicht der richtige Ort. Das Gesetz muss aber zumindest klarstellen, welchen Zielen eine solche sicherheitspolitische Entscheidung Rechnung tragen soll, ja? Etwa: Dürfen politische Vorbehalte eine Rolle spielen oder nicht? Ist es eine rein technisch-ökonomische Entscheidung oder nicht? Wie sind die einzelnen Parameter zueinander? Das müsste vergesetzlicht werden im Sinne eines entweder Negativkatalogs an den Ausschluss der Vertrauenswürdigkeit und/oder vielleicht in Kombination an einen Positivkatalog an die Antwort der technischen Leistungsfähigkeit resilient gegen bestimmte Formen der Angriffe zu sein. Und wenn das Gesetz das ausbuchstabiert hat in den wesentlichen Grundparametern, könnte man dann mit einer Verordnungsermächtigung oder vielleicht mit einer Ermächtigung zu einer Verwaltungsvorschrift im qualifizierten Verfahren die technischen Details regeln. Ich verweise als Anregung […] auf das Bundes-Immissionsschutzgesetz, Verwaltungsvorschriften nach § 48 Bundes-Immissionsschutzgesetz, da werden technische Anleitungen zwischen Ministerialverwaltungen und Sachverstand aus Wirtschaft und gesellschaftlichen Gruppen gemeinsam ausgearbeitet, die dann wiederum mit einer relativen Außenwirkung ausgestattet wurden…

Vors. **Andrea Lindholz** (CDU/CSU): Jetzt ist Feierabend. Jetzt hören wir nichts mehr.

SV **Prof. Dr. Klaus F. Gärditz** (Rheinische Friedrich-Wilhelms-Universität Bonn): Geht's jetzt wieder, Frau Vorsitzende?

Vors. **Andrea Lindholz** (CDU/CSU): Ja.

SV **Prof. Dr. Klaus F. Gärditz** (Rheinische Friedrich-Wilhelms-Universität Bonn): Ich glaube, ich brauche nur den letzten Satz wiederholen, als das Bild hing. Eine Anregung wäre vielleicht mal einen Blick in das Bundes-Immissionsschutzgesetz und die dortigen technischen Anleitungen zu werfen, das sind Verwaltungsvorschriften, die zwischen Ministerialverwaltungen […] und Sachverstand aus gesellschaftlichen Gruppen gemeinsam ausgehandelt werden und die dann von der Rechtsprechung mit einer relativen Außenwirkung ausgestattet wurden. Da kann man dann die technischen Details regeln, wenn man erstmal die wesentlichen politischen Parameter fixiert hat. Ich glaube aber auch, im Interesse der Bundesverwaltung wäre, wenn sie sich auf eine rechtssichere und ausreichend bestimmte Grundlage verlassen könnte, die juristisch einwandfrei durchsetzbar ist. Herzlichen Dank.

Vors. **Andrea Lindholz** (CDU/CSU): Vielen Dank. Ich weiß nicht, an welcher Leitung es liegt. Nach zwei Stunden macht das System Schluss. So, Herr Atug bitte.

SV **Manuel Atug** (AG KRITIS, Bonn): Danke schön. Vielleicht noch an Herrn Schallbruch, bevor ich die Fragen beantworte, eine Anmerkung: Man muss kein Jurist sein, um zu verstehen, dass § 4 BSI-Gesetz natürlich eine Meldepflicht beinhaltet. Die Schwachstellen sind zu melden an KRITIS-Betreiber und andere beispielsweise, aber es geht um Ausnahmen, ja? § 4 Absatz 4 dürfte Ihnen ja auch geläufig sein. Da ist eine Ausnahme bei Geheimhaltungsbedarf. Und genau um diese Ausnahmen geht es. Das ist das Problem, weniger die Regelung.

So, Frau Anke Domscheit-Berg hatte gefragt wegen dem IT-Sicherheitskennzeichen. 70 Prozent Menschen wollen sozusagen mehr Hilfe. Das ist auch verständlich und vor diesem Hintergrund: Was bedeutet das freiwillige IT-Sicherheitskennzeichen und die freiwillige Vergabe? Kurz gesagt bedeutet es, wünsch dir was. Denn es gibt zwei Sorten von Menschen, die einen sind technikaffin, die kriegen auch ohne ein Sicherheitskennzeichen auf die Kette, herauszufinden: worum geht es eigentlich? Ist diese Komponente sicher? Will ich die kaufen oder will ich bewusst diese Sicherheitslücken aussparen und sagen: Günstig, IoT – das S in IoT steht für Sicherheit – kaufe ich hier bewusst günstig ein. Die andere Sorte ist die, die mit IT- und Technikaffinität nicht so bewandert ist, und die scheitern in der Regel schon daran, dass sie irgendwie versuchen, einen QR-Code abzufotografieren, also eine Technologie zu nutzen, um rauszufinden, welchen Sicherheitsstand diese Komponente hat. Das ist eben nicht wie ein Energielabel draufgeklebt, sondern es soll ja so eine Art QR-Code sein, und dann kann man auf der BSI-

Webseite live nachsehen, wie der Sicherheitsstand ist. Halte ich nicht für realistisch, wenn ich mich in meinem Umfeld umschaue und sage, es gibt grob diese zwei Splittergruppen. Diejenigen wird es also schlichtweg entweder sowieso nicht interessieren oder, selbst wenn sie versucht wären, interessiert zu sein, werden sie vermutlich an dem Einsatz der Technologie scheitern. Insofern ist das auch für die Nutzer nicht wirklich die Hilfe, die da gefordert wird, sondern wieder eine unausgegorene halbgare Lösung, die durchaus zu einer guten ausgestattet werden kann, aber so in der Form nicht. Für die Hersteller ist das eine schöne Lösung, weil diejenigen, die eh keinen Wert auf Sicherheit legen lassen es einfach sein und geben nicht kund, wie schlecht ihr Produkt ist. Diejenigen, die da Lust und Laune darauf haben, könnten durchaus pfiffig sein. Ich tue jetzt mal so, als wäre ich Vertriebler oder Marketingchef einer solchen Herstellerfirma und sage: Okay, liebe Produktion, wie lange wollt ihr diese Komponente mit Sicherheitspatches versorgen? Zwei Jahre? Alles klar. Ein Jahr, 10 Monate, wenn wir das Ding mit dem IT-Sicherheitskennzeichen versehen, dann labeln wir das weg. Restverkäufe gehen dann halt ohne weiter. Die nächsten 10 Jahre, dann verkaufen wir genauso digitalen Elektronikschrott wie alle anderen – und das fällt noch nicht mal auf. In der Hauptzeit haben wir das mit diesem Label verkauft, in der Zeit danach halt dann einfach ohne, weil wir dann sagen: Wollen wir nicht mehr.

Dann war ja noch die Anmerkung, wenn man das auf Aktenlage einreicht und das BSI auf Aktenlage prüft, ist das eine geeignete Grundlage? Die Anmerkung war ja, dass diese medizinischen Geräte Schwachstellen beinhalten, die auf Papierbasis nicht gefunden worden wären von der Frau Dietrichs oder so. Im BSI gab es diese Prüfung, die hatten ungefähr 157 Schwachstellen gefunden. Genau. Reicht das aus oder bringt das was, eine solche geeignete Grundlage? Nö, auch hier ist ja wie bei den kritischen Komponenten das Ziel unklar. Die Erhöhung der IT-Sicherheit ist es jedenfalls nicht, denn sie hat ja selber schon korrekt dargelegt, auf Papierlage kann man eben nicht Schwachstellen sinnvoll finden, höchstens prozessuale eklatante Fehler. Wir haben ja jetzt beispielsweise eine Papierlagenanalyse des IT-Sicherheitsgesetzes 2.0 alle gemacht und alle Sachverständigen kommen zu Fehlern, weil eben strategisch prozessual Fehler bestehen. In der Detaildiskussion hängt es ja immer von der Detailimplementierung ab. Bei Kryptographie ist es beispielsweise so, dass selten der Algorithmus selber kaputt oder defekt oder schlecht ist, sondern in der Regel die Implementierung fehlerhaft ist. Und genau hier ist der Casus knacksus, ich habe auf der einen Seite die Papierlage, die sieht dann vielleicht schön aus, auf der anderen Seite vielleicht eine schlechte Implementierung, die wird dadurch einfach nicht besser, wenn sie auch noch ein Label kriegt: Hey, dieses Produkt ist sogar IT-sicher.

Zur Evaluierung. Das Argument der Bundesregierung, dass das IT-SiG 1.0 eh nicht mehr gelten würde und ersetzt wird und dass das rückwirkend nicht sinnvoll ist, ob doch, dann sage ich: Unbedingt ist das sinnvoll, ja? § 8a und 8b BSI-Gesetz für Kritische-Infrastruktur-Betreiber wurden ja gar nicht so stark verändert. Die haben ja nur minimale Veränderungen. Selbst, wenn man jetzt sagen würde, man prüft diese KRITIS-Verordnung, die anhängige, nicht und die Details da drin oder die anderen Dinge nicht, kann man doch zumindest den § 8a und b vorgezogen evaluieren, um zu sagen, wir legen den Fokus auf genau das, was im IT-Sicherheitsgesetz 1.0 relevant war, nämlich Kritische Infrastrukturen und evaluieren, ob und wie diese Wirkmittel und Maßnahmen, die wir da definiert haben, funktionieren oder eben nicht funktionieren. Da verweise ich wieder auf meine Anmerkung zum Demming-Circle und zum Feedback-Kreis.

Bei Audits ist es immer so, wenn Sie eine Prüfung machen, und das gibt auch das BSI übrigens selber vor in ihrem IT-Grundschutz in der Methodik, in der ISO 27001 weltweit international, man schaut in einem Audit immer auf einen Zeitraum in der Vergangenheit, in der Regel ein Jahr. Denn Sicherheit ist ein Prozess und kein Zustand. Und diesen Prozess möchte man gelebt sehen. Das heißt, man schaut sich ein Jahr Historie mit Stichproben an und prüft, ob das Sinn oder Unsinn war, was man da umgesetzt hat, ob man die Maßnahmen eingehalten hat und ob man die Vorgaben, die man sich gemacht hat, eben eingehalten hat. Das BMI hat die Vorgabe nicht eingehalten, Evaluierungen durchzuführen, und jetzt will es noch irgendwie erklären, dass der Zeitraum 2015 bis 2019 beispielsweise vom § 8a und 8b irgendwie nicht evaluiert werden

müsste. Kann ich überhaupt nicht verstehen.

Vors. **Andrea Lindholz** (CDU/CSU): Herr Atug, können Sie sich ein bisschen kürzer fassen, bitte?

SV **Manuel Atug** (AG KRITIS, Bonn): Okay. Also, der Punkt ist, es macht keinen Sinn, wenn man es nicht evaluiert. Man kann es auch vorziehen.

Dann komme ich zu den Fragen von Frau Rößner. Das Krankenhaus mit 500.000 Leuten fällt unters IT-Sicherheitsgesetz 1.0, war die Anmerkung. Korrekterweise sind KRITIS-Betreiber alle Krankenhäuser, die im Detail jetzt aus der KRITIS-Verordnung 30.000 vollstationäre Behandlungen im Jahr hatten. Das ist die genaue Definition, egal ob es eine Privatklinik ist oder sie in der Pampa steht. Und was sich an dieser Grenzziehung verbessert hat: Ja, nichts. Weil die wurde eben nicht evaluiert oder aktuell angedachte Änderungen, zum Beispiel für die Siedlungsabfallentsorgung, müssen ja einfließen, das heißt, es wird ein Update dieser anhängenden KRITIS-Verordnung geben, in der genau diese Schwellenwerte definiert sind. Pauschal 500.000 Personen als Kenngröße. Die wird also angepasst werden. Ob da eine Evaluierung reinstreut oder nicht, keine Ahnung, entzieht sich meiner Kenntnis. Selbst wenn da etwas angepasst wird: Ja, es ist da, wenn es da ist, wird es vermutlich geben. Auch da wird niemand einbezogen, es wird nicht öffentlich unterstützt oder das Know-how der Experten eingeholt.

Dann war die Frage: Was sind Unternehmen im besonderen öffentlichen Interesse – UnböfI abgekürzt? Ja, das ist ein sinnloses deutsches Kleinteiligkeitskonstrukt, in dem aktuell keiner genau weiß, wer und warum UnböfI wird oder auch nicht. Es gibt drei grobe Einteilungen: Unternehmen, die in der Rüstungsindustrie tätig sind, also Militärnahes machen. Das gehört aus Sicht der AG KRITIS eher unter den Blickwinkel der nationalen Sicherheit, weniger unter den Blickwinkel KRITIS-light. Dann gibt es eben die Unternehmen, die unter der Störfallverordnung verortet sind. Ja, da stellt sich mir die Frage oder auch uns als AG KRITIS: Die müssten doch eigentlich alle besonders irgendwie KRITIS mit Schwellenwert sein …

Vors. **Andrea Lindholz** (CDU/CSU): Herr Atug, ich muss jetzt noch mal kurz unterbrechen. Könnten Sie jetzt bitte zum Punkt kommen? Die Frage bezog sich konkret auf die Unternehmen, die die Impfdosen ausliefern. Wir haben jetzt 16:20 Uhr und noch einen Sachverständigen.

SV **Manuel Atug** (AG KRITIS, Bonn): Ich hatte aufgeschrieben: Was sind UnböfI und fallen die da drunter?

Vors. **Andrea Lindholz** (CDU/CSU): Nein, sie hat ganz klar gefragt, warum diese Unternehmen, die den Impfstoff liefern, warum die da drunter fallen unter die Kritischen Infrastrukturen.

SV **Manuel Atug** (AG KRITIS, Bonn): Das war die letzte Frage, die ich notiert habe, dann beantworte ich das. Fallen COVID-19-Impfstoffhersteller da drunter? Ja, wenn Sie über dem Schwellenwert der BSI-KRITIS-Verordnung sind. Ansonsten nein. Und daher wäre eine Evaluierung schön gewesen, ob und wie man das anpassen müsste, um diese Fragestellung so zu adressieren, dass man sagt, sind die jetzt alle relevant oder will man da einen Schwellenwert anpassen? Adressieren wir die damit vollständig oder nur die ganz Großen? Die werden adressiert unter der KRITIS-Verordnung, nicht unter UnböfI. Danke.

Vors. **Andrea Lindholz** (CDU/CSU): So, und dann noch Herr Artz bitte.

SV **Sebastian Artz** (Bitkom e. V., Berlin): Ja, in Anbetracht der Zeit, zwei Punkte die ich gern noch mal hervorheben möchte. Einerseits bezüglich der legislativen Interdependenz, die angesprochen wurde, wonach gefragt wurde: Was gibt es für Beispiele? Hier ist natürlich vor allem wie bereits angesprochen auf die neue NIS-Richtlinie zu verweisen, die jetzt eben auch auf dem Tisch liegt, wo wir Unterscheidungen in essential und important entities haben, was natürlich Fragen aufwirft, inwieweit das eben vereinbar ist mit er aktuellen Unterscheidung im IT-Sicherheitsgesetz zwischen KRITIS und Unternehmen im besonderen öffentlichen Interesse. Und da muss wirklich auch noch mal genau draufgeschaut werden, weil wir aktuell natürlich gerade, was die definitorische Ungenauigkeit von kritischen Komponenten angeht, sehr stark auf den TK-Sektor schauen. Im Endeffekt ist es aber so, dass wir jetzt mit diesem Gesetzesvorhaben wirklich auch die Leitplanken für die nächsten Jahre für die gesamte Wirtschaft setzen, das heißt, kritische Komponenten, wenn wir das nicht ausreichend rechtssicher auch gestalten, dann werden wir viele, viele Fragen aufwerfen in anderen Sektoren, nicht nur KRITIS,

sondern eben auch gerade im Bereich der Unternehmen im besonderen öffentlichen Interesse. Und es ist eben sicherlich noch mal zu erwähnen, dass wir beim IT-Sicherheitsgesetz aktuell nur einen Teilausschnitt des Gesamtkonstrukts vorliegen haben. Gerade wenn wir uns anschauen, dass beispielsweise die Unternehmen im besonderen öffentlichen Interesse die Garantieerklärung, aber eben auch das IT-Sicherheitskennzeichen, erst im Nachgang durch entsprechende Rechtsverordnungen und Allgemeinverfügungen ausgestaltet werden. Deswegen ist es da umso wichtiger, dass im Gesetz jetzt schon festgeschrieben wird, dass die Wirtschaft entsprechend angehört und beteiligt wird, damit wir diesen gemeinschaftlichen und kooperativen Ansatz auch weiter fortführen können. Das hatte Herr Dr. Herpig bereits angesprochen und das möchte ich gern an der Stelle auch noch mal sekundieren, dass Sicherheit eben keine Einbahnstraße ist und dass wir eine faire Lastenteilung brauchen, sodass wir effektiv alle gemeinsam auf das Ziel einzahlen, die IT-Sicherheit in Deutschland in den Kritischen Infrastrukturen zu steigern.

Zu guter Letzt möchte ich gern noch auf die Frage von Herrn Hartmann eingehen, der sich auf den § 10 Absatz 6 bezog, wo wir eben genau diese Problematik haben. Dadurch, dass wir IT-Produkte als Einzel- oder miteinander vernetzte Hardwareprodukte verstehen, im § 2 Absatz 9a oder b ist es, glaube ich, definiert, dass wir da natürlich diese Unschärfe haben, was sind im Endeffekt wirklich kritische Komponenten? Und dass wir mit Blick auf § 10 Absatz 6 jetzt natürlich die Frage haben, inwieweit dieser bestimmende Ansatz, dass das BMI eben nach Anhörung, aber ohne im Einvernehmen mit der Wirtschaft, bestimmte Prozesse zur Interoperabilität, zur Offenhaltung von Schnittstellen und zur Einhaltung etablierter technischer Standards bestimmen soll. Hier muss ganz klar darauf geachtet werden, dass das im Einvernehmen mit der Wirtschaft geschieht und nicht einfach bestimmend oben drüber gestülpt, weil wir wirklich hier die faire Lastenteilung brauchen und ich auch noch mal an der Stelle wirklich betonen möchte, dass die Wirtschaft gesprächs- und dialogbereit ist und sich wirklich wünscht, in diese ganzen Prozesse mit einbezogen zu werden. Gerade, weil wir hier natürlich auch technische Standards setzen, die wir international und europäisch skalieren müssen, damit wir unsere exportorientierte Wirtschaft stärken. Das vielleicht zum Abschluss noch von meiner Seite.

Vors. **Andrea Lindholz** (CDU/CSU): Vielen Dank, Herr Artz. Dann darf ich mich noch mal bei allen Sachverständigen und Kollegen bedanken und würde die Anhörung jetzt hiermit schließen und wünsche Ihnen noch eine gute restliche Woche.

Schluss der Sitzung: 16:24 Uhr

Andrea Lindholz, MdB
Vorsitzende

bitkom

Auf einen Blick

IT-Sicherheitsgesetz 2.0

Bitkom-Bewertung

Bitkom unterstützt die Zielsetzung der Bundesregierung, IT-Sicherheit zum Schutz der a) Kritischen Infrastrukturen, b) Bundesverwaltung und c) Verbraucher zu gewährleisten. Allerdings erachtet Bitkom die angedachte Umsetzung in wesentlichen Punkten als **kritisch und überarbeitungsbedürftig**.

Das Wichtigste

- **Unzureichende Festlegung auf Schutzziele**
  Bitkom fordert ein klares, dem IT-SiG 2.0 vorangestelltes Konzept zu den Schutzzielen Vertraulichkeit, Integrität und Verfügbarkeit sowie die konsistent darauf ausgerichtete, gesetzgeberische Umsetzung. Nur auf Basis eines klaren Zielverständnisses und einer nachvollziehbaren Evaluierung des IT-SiG 2015 lassen sich geeignete Schutzmaßnahmen definieren. Diese sind dabei im Hinblick auf Innovationsfreundlichkeit, Investitionsschutz und Rechtssicherheit auf ihre Tauglichkeit zu bewerten. Sicherheit und Schutz sind Zustände, die erreicht und gehalten werden müssen. Dies kann nicht statisch geschehen, sondern die Maßnahmen, die Sicherheit und Schutz bewirken, bedürfen einer permanenten Wirksamkeitsprüfung, Anpassung und Weiterentwicklung.

- **Wenig zielgerichtete Regulierung**
  Als unmittelbare Folge der fehlenden Konkretisierung von Schutzzielen wirkt das Gesetz inhaltlich überdehnt. Dies gilt sowohl für den sich zwischen BSI und den Sicherheitsbehörden abzeichnenden Interessenskonflikt, als auch für den nach wie vor zu unbestimmten Begriff der Vertrauenswürdigkeit. Der Schutzbedarf ist in erster Linie etwas technisch-agnostisches und bedarf einer regel- und kritikalitätsbasierten Prüfung (und Zertifizierung). Anders als überprüfbare technische Kriterien sind Garantieerklärungen ein politisch motiviertes Instrument, ohne in der Umsetzung ausreichend Rechtssicherheit zu gewährleisten. Dies mag zwar sicherheitspolitisch gewollt sein, Bitkom lehnt die jetzige Ausgestaltung jedoch ab.

- **Fokussierung der Kompetenzen von BSI und BMI erforderlich**
  Betreiber kritischer Infrastrukturen und auch Unternehmen im besonderen öffentlichen Interesse haben die Hoheit über ihre Prozesse, Ausstattungen und Geschäftstätigkeit. Bitkom lehnt technische Zugriffs- und Weisungsbefugnisse des BSI ebenso ab, wie pauschale Anordnungsbefugnisse des BMI. Dabei wird mit der erstmaligen Nennung von Interoperabilität eine eigentlich gestalterische Maßnahme mit Visionspotenzial zur langfristigen Steigerung der IT-Sicherheit im Gesetzestext in Betracht gezogen. Weshalb der Gesetzgeber diesen Punkt starr und bestrafend anstatt stimulierend ausgestaltet, erschließt sich Bitkom nicht.

- **Mangelnde Einbindung der Wirtschaft**
  Eine rechtzeitige Beteiligung der Wirtschaft im Gesetzgebungsverfahren ist unabdingbar. Bitkom stellt fest, dass bereits zum wiederholten Male Fristen zur Stellungnahme gesetzt werden, die eine der volkswirtschaftlichen Bedeutung des Themas angemessene Befassung nicht zulassen und der Betroffenheit der Wirtschaft nicht gerecht werden. Während einer laufenden Frist zur Stellungnahme einen wesentlich abgeänderten, nicht final abgestimmten Entwurf herauszugeben und eine 27-stündige Frist zur Kommentierung anzusetzen, ist absolut inakzeptabel.

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
19(4)741 A

bitkom

Stellungnahme

zum Entwurf für ein zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0)

10.12.2020

Bitkom
Bundesverband
Informationswirtschaft,
Telekommunikation
und Neue Medien e.V.

Sebastian Artz
Referent IT-Sicherheit
s.artz@bitkom.org

Albrechtstraße 10
10117 Berlin

Präsident
Achim Berg

Hauptgeschäftsführer
Dr. Bernhard Rohleder

Vorwort

Das Bundesministerium des Innern, für Bau und Heimat (BMI) hat am 02.12.2020 einen nicht abgestimmten Diskussionsentwurf eines zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-SiG 2.0) vorgelegt und bis zum 09.12.2020 um Stellungnahme gebeten. Kurz vor Ablauf der eigens durch das BMI gesetzten laufenden Frist wurde am 09.12.2020 ein signifikant abgeänderter, nach wie vor nicht ressortübergreifend abgestimmter Referentenentwurf zirkuliert, zu dem innerhalb von 27 Stunden, bis zum 10.12.2010 um 14 Uhr, Stellung bezogen werden soll. **Ein derartiges Vorgehen ist absolut inakzeptabel.**

Angesichts der wachsenden Bedeutung des Cyberraums und informationstechnischer Systeme in der gesamten wirtschaftlichen und gesellschaftlichen Breite, und der damit einhergehenden hybriden und sich ausweitenden Bedrohungslage, ist es grundsätzlich zu begrüßen, dass die Bundesregierung Cyber- und IT-Sicherheit verstärkt in den Blick nimmt. Es stellen sich jedoch unmittelbar daran anknüpfend richtungsweisende Folgefragen, die der Gesetzgeber unbeantwortet lässt. Aktuell fehlt dem Gesetzesentwurf ein klares Bekenntnis dazu, welche konkreten Schutzziele mit dem IT-SiG 2.0 verfolgt werden sollen. Nur auf Basis eines klaren Zielverständnisses lassen sich geeignete Maßnahmen auswählen. Dabei müssen alle Maßnahmen auf Innovationsfreundlichkeit, Investitionsschutz und Rechtssicherheit überprüft und bewertet werden.

Grundprämisse für die Gewährleistung eines hohen Cybersicherheitsniveau ist, dass alle relevanten Stakeholder, von Betreibern über Hersteller bis hin zu staatlichen Stellen, auf vertrauensvoller und kooperativer Basis an einem Strang ziehen und ihre jeweilige Verantwortung innerhalb des Gesamtökosystems übernehmen. Eins muss ins andere greifen, denn im Cyberraum beginnen die Gefahren am schwächsten Glied in der Kette. Hierzu bedarf es des fairen und innovationsstimulierenden Wettbewerbs, basierend auf gleichen Regeln für gleiche Dienste und Angebote sowie der Vielfalt von Technologien und Anbietern. Die Relevanz eines technologieneutralen Ansatzes ist dabei von fundamentaler Bedeutung. Für alle Hersteller – ganz gleich welcher Produkte und Angebote sowie unabhängig ihrer Herkunft – sollten die gleichen produkt- und angebotsspezifi-

schen Prüfkriterien, Regeln und Verfahren gelten. Dabei darf sich das Zusammenwirken mitnichten nur auf die nationale Ebene beschränken. In einem starken, vereinten und zukunftsgerichteten Europa muss Cyber- und IT-Sicherheit global, mindestens aber gesamteuropäisch, gedacht werden. Andernfalls würden selbst gut gemeinte Maßnahmen als Sammelsurium nationaler Alleingänge ohne signifikante Steigerung des Sicherheitsniveaus ins Leere laufen. Die Kohärenz der deutsch-europäischen Cybersicherheitsausrichtung ist für Bitkom von zentraler Bedeutung.

Vor diesem Hintergrund muss Bitkom die folgenden erfolgskritischen Punkte im aktuellen Entwurf des IT-SiG 2.0 zur Sprache bringen:

Legislative Interdependenzen im Gesamtkontext und generelle Verfahrenskritik

Komplexität ist der größte Feind von Sicherheit. Mit dem wechselseitigen Zusammenspiel aus

- Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG (2.0)),
- Europäische Richtlinie zur Gewährleistung einer hohen Netzwerk- und Informationssicherheit (NIS-Richtlinie (2.0)),
- Verordnung zur Bestimmung Kritischer Infrastrukturen nach BSIG (KRITIS-V),
- Telekommunikationsgesetz (TKG),
- Telekommunikationsmodernisierungsgesetz (TKG-E),
- Katalog von Sicherheitsanforderungen für das Betreiben von Telekommunikations- und Datenverarbeitungssystemen sowie für die Verarbeitung personenbezogener Daten nach § 109 TKG (insb. Anhang II),
- Liste der kritischen Funktionen für öffentliche Telekommunikationsnetze und -dienste mit erhöhtem Gefährdungspotenzial als Ergänzung zur Anlage 2 des Katalogs von Sicherheitsanforderungen nach § 109 Abs. 4 TKG,
- EU Cybersecurity Act (CSA, Verordnung EU 2019/881),
- verschiedener (CSA-)Zertifizierungsschemata,
- einzelner Technischer Richtlinien des BSI und
- weiterer noch zu spezifizierender Rechtsverordnungen

existiert eine multidimensionale Gemengelage, bei der es essenziell ist, dass sich alle Elemente nahtlos zusammenfügen. Mit der parallelen Überarbeitung sowie der erstmaligen Anfertigung einiger der genannten Gesetzestexte besteht grundsätzlich das inhärente Risiko, ein dysfunktionales Gesamtkonstrukt zu schaffen. Es ist dringend geboten, die Konsolidierung der Regelungsgegenstände eng und widerspruchsfrei zu fassen und Redundanzen auszuschließen. Die verzögerte Veröffentlichung der

verschiedenen Gesetzestexte hat Zweifel an einem konsistenten Gesamtvorgehen genährt, mit negativen Konsequenzen für die Erwartungs-, Investitions-, und Rechtssicherheit in der Wirtschaft. Das wiederholte Vorlegen eines inoffiziellen und an zentralen Stellen unvollständigen »Diskussionsentwurfs« eines TKG-E hat dies ebenso sehr verdeutlicht wie der am 2. Dezember vorliegende, nicht abgestimmte Gesetzestext eines IT-SiG 2.0. Trotz der enormen Relevanz der Gesetzesinhalte und ungeachtet einzelner im Vorfeld publik gewordener Referentenentwürfe wurde lediglich eine Kommentierungsfrist von einer Woche gewährt, nachdem ursprünglich sogar nur eine 2,5 arbeitstägige Frist angesetzt wurde. Unmittelbar vor Ablauf der vom BMI eigens nach außen getragenen Kommentierungsfrist wurde dann ein wesentlich abgeänderter, nicht im Änderungsmodus nachvollziehbarer Referentenentwurf, mit einer Kommentierungsfrist von 27 Stunden, an die unmittelbar betroffene Wirtschaft übermittelt.

Der Bundesregierung und den Bundesministerien ist es in einer zweijährigen Debatte nicht gelungen, einen aus ihrer Sicht konsistenten Referentenentwurf zu entwickeln. Das federführende BMI hat es zudem versäumt, eine frühzeitige, sachgerechte Beteiligung der Betroffenen zu ermöglichen. Dies wird der Betroffenheit der gesamten Wirtschaft in keiner Weise gerecht.

Vernachlässigung der kooperativen und dialogbasierten Erfolgskomponente zur Steigerung der IT-Sicherheit

Transparenz ist eine wesentliche Grundlage für Vertrauen. Dies setzt einen kooperativen Ansatz mit klar definierten Regeln für alle Seiten voraus. Der Gesetzgeber hat mit dem IT-SiG 2015 einen aus Sicht des Bitkom passenden regulatorischen Rahmen gesetzt und ca. 2.000 Betreiber kritischer Infrastrukturen sowie deren Zulieferer verpflichtet, ein ISMS (Informationssicherheitsmanagementsystem) einzuführen bzw. das bestehende zu ergänzen. Die dort für Unternehmen bzw. Behörden geltenden Regelungen sind regelmäßig zu evaluieren und auf Basis von Erfahrungen und Risiken zu überarbeiten. Bitkom erwartet eben diese Best Practice auch von Gesetzgeber, d. h. die Evaluation und risikogemäße Weiterentwicklung des IT-SiG. Mit dem IT-SiG 2.0 wird nun allerdings der regulative Rahmen ausgeweitet, ohne dass den betroffenen Branchen der gesetzgeberische Handlungsbedarf aufgezeigt wurde. Damit wird die erfolgskritische kooperative, gemeinschaftliche Herangehensweise zugunsten eines verstärkt bestimmenden Ansatzes vernachlässigt. Zweckdienlicher wäre es, die vertrauensvolle Zusammenarbeit im Rahmen der bereits etablierten und geschätzten Initiativen des UP KRITIS sowie der Allianz für Cyber-Sicherheit zu stärken und die dortigen Erkenntnisse über entsprechende Feedback-Schleifen verstärkt im Gesetzgebungsprozess zu berücksichtigen. Aus unserer Sicht muss die nachvollziehbare Evaluierung des IT-SiG 2.0 im Vorfeld der Ausarbeitung eines

IT-SiG 3.0 verpflichtend gemacht werden. Gleiches gilt für die Ausgestaltung künftiger Rechtsverordnungen. Bereits bestehende Gesprächskanäle können hier problemlos und ressourcenschonend genutzt werden. Ein Mangel an Koordination manifestiert sich dabei auch auf europäischer Ebene.

Die sicherheitsfördernde Hebelwirkung legislativer Harmonisierung auf europäischer Ebene wird unzureichend berücksichtigt

Durch die Verzögerung auf deutscher Seite kommt es aktuell zur parallelen Überarbeitung des IT-SiG und dessen europäischen Pendant, der NIS-Richtlinie. Während das IT-SiG 2015 im Vorfeld der Verabschiedung der NIS-Richtlinie im Jahr 2016 als Musterbeispiel herangezogen werden konnte, besteht aktuell keine Abstimmung beider Verfahren, so dass – obwohl beide Vorhaben auf die Steigerung des Schutzes kritischer Infrastrukturen abzielen – die parallel stattfindenden Überarbeitungen in Silos stattfinden und der übereinstimmenden Zielsetzung zuwiderlaufen. Unsere Sorgen beruhen konkret auf drei Vorhaben des deutschen Gesetzgebers:

1. Einführung einer neuen nationalen Sonderkategorie: »Unternehmen von besonderem öffentlichen Interesse« (§ 2 Abs. 14 in Verbindung mit § 8f BSIG-E)
2. Ausweitung der nationalen KRITIS-Sektoren auf den Bereich der »Siedlungsabfallentsorgung« (§ 2 Abs. 10 BSIG-E)
3. Einführung eines freiwilligen nationalen IT-Sicherheitskennzeichens (§ 9c BSIG-E)

Entgegen der aktuellen Ausgestaltung müssen die genannten Vorhaben auf das elementar wichtige Ziel europäischer Harmonisierung im Bereich Cyber- und IT-Sicherheit einzahlen. Andernfalls sind negative wettbewerbsrechtliche Implikationen für den Wirtschaftsstandort Deutschland absehbar, im schlechtesten Fall auch durch nicht abgestimmte Doppelregulierungen. Dies gilt insbesondere für die neugeschaffene Sonderkategorie »Unternehmen von besonderem öffentlichen Interesse«, die europa-weit ihresgleichen sucht. Aus dem Grund ist von dieser einzelstaatlichen Quasi-KRITIS-Kategorie abzuraten.

Mit Blick auf das Ziel, die Sicherheit informationstechnischer Systeme zu steigern, kann es nicht im Interesse der Politik sein, das IT-SiG 2.0 im kommenden Jahr erneut aufzuschnüren und – im schlechtesten Fall erneut ohne nachvollziehbare Evaluierung – mit einem IT-SiG 3.0 fortzufahren, nur um die sich bereits abzeichnende Fehlabstimmung mit der NIS-Review wieder zu beheben. Dies hätte zweifelsohne negative Auswirkungen auf den Wirtschaftsstandort Deutschland und auf die mit dem IT-SiG 2.0 ohnehin schon induzierte Rechtsunsicherheit für die Unternehmen, wie der nachfolgende Punkt aufzeigt.

Definitorische Ungenauigkeit von verwendeten Begrifflichkeiten und induzierte Rechtsunsicherheit

Die definitorische Ungenauigkeit manifestiert sich insbesondere in drei Begrifflichkeiten:

1. Unternehmen im besonderen öffentlichen Interesse (§§ 2 Abs. 14 und 8f BSIG-E)
2. IT-Produkte (§ 2 Abs. 9a BSIG-E)
3. Kritische Komponenten (§ 2 Abs. 13 BSIG-E)

Während IT-Produkte als »*Softwareprodukte sowie alle einzelnen oder miteinander verbundenen Hardwareprodukte*« definiert werden, sind Kritische Komponenten »*[…] IT-Produkte, die in Kritischen Infrastrukturen eingesetzt werden, die von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit dieser IT-Produkte zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Funktionsfähigkeit Kritischer Infrastrukturen oder zu Gefährdungen für die öffentliche Sicherheit führen können, wenn diese*

1. *auf Grund eines Gesetzes als solche bestimmt werden oder*
2. *auf Grund eines Gesetzes als kritisch bestimmte Funktionen realisieren, aus denen nach dem Gesetz kritische Komponenten abgeleitet werden können*«.

Während die Definition von IT-Produkten weiterhin zu viel Interpretationsspielraum lässt, ist der unternommene Versuch, Kritische Komponenten regulatorisch besser zu fassen, grundsätzlich zu begrüßen. Aus Gründen der Rechts-, Investitions- und Planungssicherheit muss die Definition Kritischen Komponenten aber aus dem Gesetz selbst heraus und hinreichend genau erfolgen. Der Entwurf wird dieser Anforderung aktuell nicht gerecht. Dabei begrüßt Bitkom grundsätzlich den in § 2 Abs. 13 Nr. 2 enthaltenen Ansatz, Kritische Komponenten über kritische Funktionen zu definieren. Allerdings enthält die aktuelle Formulierung in § 2 Abs. 13 Nr. 2 zu viele Unwägbarkeiten. Was genau ist mit der Formulierung »auf Grund eines Gesetzes« gemeint? Welche(s) Gesetz(e)? Wird es eine Anhörung und Beteiligung der Wirtschaft geben? Die Gesetzesbegründung gibt Aufschluss: »*Für den Bereich der Kritischen Infrastrukturen, die ein öffentliches Telekommunikationsnetz betreiben oder öffentlich zugängliche Telekommunikationsdienste erbringen, legt beispielsweise § 109 Absatz 6 des Telekommunikationsgesetz fest […]. Komponenten, welche die in dem Katalog von Sicherheitsanforderungen aufgeführten Funktionen realisieren, sind damit kritische Komponenten im Sinne des § 2 Absatz 13 BSIG.*« Bitkom fordert eine entsprechende Konkretisierung unmittelbar in § 2 Abs. 13 Nr. 2 vorzunehmen. Die hinreichend genaue, rechtssichere Definition Kritischer Komponenten ist zwingend erforderlich. Dies gilt umso mehr für § 2 Abs. 13 Nr. 1, wo aktuell eine direkte, gesetzliche Be-

stimmung (siehe Gesetzesbegründung) kritischer Komponenten vorgesehen ist. Bitkom lehnt die in § 2 Abs. 13 Nr. 1 vorgesehene, gesetzliche Bestimmung kritischer Komponenten ab. Es bedarf zwingend an Transparenz und unmittelbaren Beteiligungsmöglichkeiten für die durch die Entscheidung Betroffenen. Es sollte zusätzlich klargestellt werden, dass nur speziell für den Einsatz in Kritischen Infrastrukturen hergestellte Kritische Komponenten – identifiziert vor allem durch die Betreiber selbst – als eben solche gelten können. Agnostische IT-Produkte, deren Verwendung sich nicht ausschließlich auf KRITIS-Bereiche beschränkt, müssen zunächst ausgeklammert sein. Vor diesem Hinter-grund ist es zu begrüßen, dass gemäß § 2 Abs. 13 Satz 2 Einschränkungen der vorgesehenen Regelung möglich erscheinen.

Die Einordnung und Bewertung Kritischer Komponenten im legislativen Gesamtkontext des IT-SiG 2.0 wird ab Seite 11 fortgeführt.

Kompetenzerweiterung für das Bundesamt für Sicherheit in der Informationstechnik (BSI)

Bitkom begrüßt die personelle Aufwertung und finanzielle Stärkung des BSI. In der Vergangenheit konnten wir unter dem Dach des Bitkom auf die vertrauensvolle Zusammenarbeit und den fachlichen Dialog mit den Spezialisten des BSI zählen, um die Cyber- und IT-Sicherheit in Deutschland gemeinsam voranzubringen. Wir freuen uns darauf, den kooperativen Austausch in Zukunft mit einem personell gestärkten BSI weiter zu intensivieren. Gleichzeitig gibt es im Zuge der Änderungen des BSIG wesentliche Aspekte, die es kritisch hervorzuheben gilt:

- Die Kompetenzausweitung und der damit einhergehende massive Personalaufbau aufseiten des BSI lassen befürchten, ja sogar erwarten, dass die Behörde über Jahre an Wachstumsschmerzen kranken wird und die hochgesteckten Ziele kurz- und mittelfristig nicht zu erreichen vermag. Zudem führt die Kombination von Aufgaben unterschiedlicher Zielrichtung (objektive Sachverhaltsaufklärung zu präventiven und repressiven Zwecken einerseits und einseitig zielgerichtete Durchsetzung von Interessen von Verbrauchern als einer bestimmten gesellschaftlichen Gruppe andererseits) zu nicht auflösbaren Interessenskonflikten und erscheint aus diesem Grund verfassungsrechtlich problematisch. Die Neupositionierung des BSI als starke Aufsichtsbehörde mit weitreichenden Eingriffsmöglichkeiten und zusätzlichen Weisungsbefugnissen lässt außer Acht, dass viele der vorgesehenen zusätzlichen Aufgaben des Bundesamts im Kompetenzbereich qualifizierter vertrauenswürdiger Unternehmen und Institutionen liegen. Daneben ist es zurückzuweisen, dass das BSI einzelnen Unternehmen technische Zugriffs- und Weisungsbefugnisse erteilen darf (bspw. gemäß

§ 7c BSIG-E). Im Sinne einer effizienten Aufgabenteilung sollte das BSI nicht in bewährte privatwirtschaftliche Prozesse eingreifen oder sich diese komplett zu eigen machen. Cybersicherheit ist eine Querschnittsaufgabe und muss horizontal wie vertikal gestärkt werden. Die Bündelung von möglichst vielen Kompetenzen auf staatlicher Seite trägt dieser Querschnittslogik nicht im ausreichenden Maße Rechnung und dämpft den so wichtigen Aufbau von IT-Expertise in der wirtschaftlichen Breite.

- Bitkom spricht sich gegen die nationale Entwicklung und Festschreibung eines Stands der Technik durch das BSI aus. Die aktuell gewählte gesetzliche Formulierung des §3 Abs. 1 Satz 2 Nr. 20 verkennt, dass sich der Stand der Technik an den Prozessen der Normung und Standardisierung orientiert, im Einvernehmen aller relevanten Stakeholder vielmehr ein Beobachtungswert der Marktanwendung darstellt und somit erst ex-post als solcher identifiziert werden kann. Somit wäre das BSI lediglich in der Lage einen zeitlich bereits überholten Näherungswert abzubilden, der dem internationalen Marktgeschehen hinterherhinkt. Die Entwicklung des Stands der Technik kann nur in enger Abstimmung und unter Einbeziehung der betroffenen Branchen sowie nach transparenten Beteiligungskriterien erfolgen. Gleiches gilt für die Ausarbeitung von Technischer Richtlinien, die internationale Normen und Standards als Ausgangsbasis verstehen müssen, nicht vice versa.

- Der Einführung eines durch das BSI verantworteten freiwilligen IT-Sicherheitskennzeichens steht Bitkom grundsätzlich positiv und offen gegenüber. Es ist jedoch zu betonen, dass ein IT-Sicherheitskennzeichen nur als ein Mosaikstein eines umfassenden Gesamtkonzepts für mehr IT-Sicherheit verstanden werden kann. Sicherheit ist ein Prozess und keine Momentaufnahme in Form eines Kennzeichens. Damit ein solches Kennzeichen seine volle Wirkkraft entfalten kann, sollte es sich auf grundlegende, produktübergreifende Schutzanforderungen beschränken und in einen Gesamtkontext eingebettet und von vornherein als europäische Lösung oder europäisch skalierbar konzipiert werden. Bei national unterschiedlichen Regelungen hingegen bestünde die Gefahr einer erheblichen Beeinträchtigung des nach dem AEUV gewährleisteten freien Waren- und Dienstleistungsverkehrs innerhalb Europas in Bezug auf IT-Produkte. Bitkom empfiehlt, innerhalb des § 9c BSIG-E auf anerkannte internationale, zumindest aber europäisch anerkannte, einheitliche Regelungen, Normen und Standards zu referenzieren. Erst wenn internationale und europäische Normen und Standards nicht existieren oder anwendbar sind, sollte auf nationale oder branchenspezifische Standards sowie Technische Richtlinien des BSI zurückgegriffen werden. Dies knüpft unmittelbar an die Ausführungen des vorherigen Absatzes an. Darüber hinaus muss es immer möglich sein, das IT-Sicherheitskennzeichen online zu veröffentlichen, nicht nur wenn die Beschaffenheit des Produktes das Anbringen nicht möglich macht. Aus

dem Grund muss § 9c Abs. 6 BSIG-E folgendem Wortlaut Rechnung tragen:
»*das IT-Sicherheitskennzeichen ist entweder auf dem jeweiligen Produkt oder dessen Umverpackung anzubringen, oder elektronisch zu veröffentlichen*.«

- Während die Untersuchung informationstechnischer Produkte und Systeme auf der Basis genereller Marktbeobachtungsbefugnisse durchaus zu begrüßen ist, überschreitet die aktuell intendierte Ausweitung der Befugnisse im Sinne der in § 7a Abs. 2 und 4 dargelegten Auskunftspflicht eine rote Linie. Derart uneingeschränkte und anlasslose Auskunftsrechte – »insbesondere auch zu technischen Details« – stehen im ungeklärten Rechtsverhältnis, wenn nicht sogar im klaren Widerspruch zum Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG).

- Im Zuge der Kompetenzausweitung des BSI ist eine klare Priorisierung der Aufgaben in Anlehnung an die noch zu definierenden Schutzziele dringlich geboten. Die im Zuge des IT-SiG 1.0 eingeführten Meldepflichten von Cybersicherheitsvorfällen haben bisher keine signifikante Verbesserung im Lagebild gebracht. Das BSI sollte der monatlichen und für die einzelnen Sektoren individuellen Erstellung von Lagebildern Priorität einräumen, bevor sich das Augenmerk auf die Erschließung neuer Kompetenzfelder richtet. Während die Festlegung auf das BSI als zentrale Meldestelle zu begrüßen ist, wird im aktuellen Gesetzesentwurf die Chance vertan, ein effizientes, harmonisiertes und dem one-stop-shop-Prinzip folgenden Meldewesens zu schaffen. Dies gilt es im Sinne des Bürokratieabbaus nachzuholen.

- Die Handhabung von Schwachstellen ist das Rückgrat zur nachhaltigen Steigerung von IT-Sicherheit in der wirtschaftlichen Breite und den Schutz informationstechnischer Systeme in Bereichen kritischer Infrastrukturen. Es braucht eine ausnahmslose Meldepflicht entdeckter Sicherheitslücken, die auch für staatliche Stellen gilt. Der aktuelle Gesetzesentwurf (§ 4b BSIG-E in Verbindung mit §§ 7, 7a, 7b, 7c und 7d BSIG-E) läuft dem allerdings zuwider. Die inhärente Intransparenz könnte zu einem Vertrauensverlust der Wirtschaft in das BSI führen. Dabei ist ein dysfunktionales Schwachstellenmanagement noch die kleinere Problemdimension. Schwerwiegender für das dem BSI entgegengebrachte Vertrauen ist der im nachfolgenden Punkt ausgeführte Interessenskonflikt mit den Sicherheitsbehörden.

Interessenskonflikt zwischen dem BSI und den Sicherheitsbehörden

Übergeordnete Zielsetzung des IT-SiG (2.0) muss die Steigerung der technischen Sicherheit von Kritischen Infrastrukturen, Unternehmen im besonderen öffentlichen Interesse und digitalen Diensten sein. Gleichzeitig wird der Versuch unternommen, das Mandat des BSI mit den Aufgaben der Sicherheitsbehörden in Einklang zu bringen. IT-Sicherheitsziele und Strafverfolgung sollten aber nicht miteinander vermengt werden, da dies weder zum Schutz unserer informationstechnischen Ziele beiträgt noch einer erfolgreichen Strafverfolgung gerecht wird. Bitkom empfiehlt, IT-Sicherheitsziele klar zu definieren und diese dem IT-Sicherheitsgesetz als Anker und Leitbild voranzustellen. Dabei empfiehlt sich die typische CIA-Security-Triangel, bestehend aus Confidentiality (Vertraulichkeit), Integrity (Integrität) und Availability (Verfügbarkeit), da diese dem Großteil der in Kritischen Infrastrukturen, in Unternehmen im öffentlichen Interesse und bei Digitalen Diensten verwendeten Risikomanagementsystemen zugrunde liegt.

Der Interessenskonflikt zwischen den Aufgaben des BSI und der Zuständigkeit der Sicherheitsbehörden manifestiert sich in den folgenden Punkten:

- Gemäß § 7b BSIG-E soll das BSI künftig zum Aufspüren von Sicherheitslücken gesetzlich legitimiert in die IT-Systeme und technischer Anlagen von kritischen Infrastrukturen eingreifen können. Die im Gesetz beschriebenen Portscans können auch als Schwachstellenscans interpretiert werden, welche als kritisch zu bewerten sind, da (zumindest) ein aktiver Schwachstellenscan das Potential hat, Dienste und Programme in Ihrer Verfügbarkeit zu stören bzw. deren Ausführung zu verhindern. Während es zwar zu begrüßen ist, dass mit Aufnahme einer »weißen Liste« eine gewisse Konkretisierung und Einschränkung der Kompetenzausweitung vorgenommen wird, können die Vorbehalte nicht vollständig ausgeräumt werden. Bitkom bewertet die aktuelle Ausgestaltung daher als problematisch; einerseits im Hinblick auf die nicht abschätzbaren und weitrechenden Konsequenzen für die Funktionstüchtigkeit der Systeme und damit für die Versorgungs- und physische Sicherheit der Bevölkerung, andererseits im Sinne eines argumentativ nicht auflösbaren Knotens der Unsicherheit. Auf welcher Basis sollen Betreiber und Unternehmen künftig Schwachstellen melden, wenn nicht gewährleistet ist, dass die Erkenntnisse und Informationen zur Beseitigung von Gefährdungslagen verwendet sondern potenziell an die Sicherheitsbehörden weitergegeben werden können? Hersteller müssen unverzüglich nach Bekanntwerden von Sicherheitslücken in ihren Produkten darüber informiert werden, um diese schnellstmöglich beheben zu können. Ein Bruch mit diesem Grundsatz würde einen Vertrauensverlust der Wirtschaft in das BSI nach sich ziehen.

- Gemäß § 7c Abs. 1 Nr. 1 kann das Bundesamt gegenüber einem Anbieter von Telekommunikationsdiensten zur Abwehr konkreter erheblicher Gefahren für die in Absatz 2 genannten Schutzziele anordnen, dass er die in § 109a Absätze 5 oder 6 des Telekommunikationsgesetzes bezeichneten Maßnahmen trifft. § 7 Abs. 3 gestattet in diesem Fall die Anordnung gegenüber dem Diensteanbieter, den Datenverkehr an eine vom Bundesamt benannte Anschlusskennung umzuleiten. Mit der ausdrücklichen Hervorhebung dieser in das Fernmeldegeheimnis eingreifenden Anordnungskompetenz erkennt der Gesetzgeber, dass ein solcher Eingriff einer ausdrücklichen Ermächtigung bedarf. Jedoch trifft diese Norm nicht die Anforderungen, die an eine Ermächtigung zum Eingriff in das Fernmeldegeheimnis zu stellen sind. Die Umleitung von Datenverkehren an eine andere Anschlusskennung ermöglicht die Kenntnisnahme der Inhalte der Kommunikation durch Dritte. Eine solche Kenntnisnahme durch Dritte steht jedoch unter einem richterlichen Vorbehalt. Zudem lässt die Vorschrift völlig offen, welchem Personenkreis die Nutzer der anderen Anschlusskennung zugeordnet sein müssen. Insoweit ist der Anwendungsbereich auf solche Nutzer zu beschränken, die den Inhalt des Datenverkehrs zur Abwehr einer konkreten Gefahr unbedingt benötigen. Im Übrigen dürfte ein Eingriff in das Fernmeldegeheimnis nur zum Schutz gleichwertiger oder höherwertiger Rechtsgüter möglich sein. Auch insoweit ist der Anwendungsbereich deutlich einzuschränken.

- Die Zweckmäßigkeit und Sinnhaftigkeit der neu eröffneten Möglichkeiten zur Kontrolle der KRITIS-Sektoren automatisierte Ermittlungen auf individueller Anwender- und Nutzerebene durchzuführen und Informationen im Sinne der in § 5c BSIG-E vorgesehenen Bestandsdatenauskunft zu sammeln und zu verarbeiten, ist unter Gesichtspunkten der Beseitigung von Störungen kritisch zu hinterfragen und abzulehnen. Die in § 5c Abs. 5 BSIG-E vorgesehene Befugnis zur Weiterleitung der in diesem Verfahren erlangten Daten an andere Behörden ist zu streichen. Dagegen ist zumindest die Aufnahme der in § 5c Abs.8 vorgesehenen Entschädigungsregelung zu begrüßen.

- Die in § 8a Abs. 1b vorgesehene Speicherfrist von 4 Jahren für die Angriffserkennung und -nachverfolgung relevanter und nicht-personenbezogener Daten ist abzulehnen und der genannte Absatz zu streichen. Andernfalls müssten Betreiber Kritischer Infrastrukturen Datenhalden von mehreren TByte vorhalten, ohne erkennbaren Mehrwert zur Steigerung der IT-Sicherheit.

Einsatz Kritischer Komponenten (nicht) vertrauenswürdiger Hersteller

Oberste Maxime ist und muss sein, dass Kritische Infrastrukturen jederzeit ein Höchstmaß an Sicherheit gewährleisten und Risiken einer technischen Kompromittierung minimiert werden. An dieser Stelle sei ausdrücklich und wiederholt betont, dass sich alle Beteiligten – sowohl Hersteller Kritischer Komponenten als auch Betreiber Kritischer Infrastrukturen – ihrer Verantwortung bewusst sind und ihren Beitrag zur gemeinsamen Zielsetzung zu leisten bereit sind. In Anbetracht der hybriden und wachsenden Bedrohungslage erachten wir den Einsatz sicherer Produkte in Bereichen Kritischer Infrastruktur für nachvollziehbar und grundsätzlich richtig. Hierbei müssen im Sinne einer Gleichbehandlung die dafür angelegten Maßstäbe transparent gemacht werden und nachvollziehbar sein. Dies lässt sich am besten als harmonisierter Ansatz auf europäischer Ebene verfolgen. Bitkom fordert deshalb eine voll umfassende Umsetzung der EU 5G-Toolbox.

Anknüpfend an die bereits genannte Forderung, die Schutzziele klar zu definieren, ist an dieser Stelle einmal mehr deutlich zu machen, dass der Schutzbedarf etwas technisch-agnostisches ist und einer regel- und kritikalitätsbasierten Prüfung unterliegen muss und auf die rechtssichere Investitionsplanbarkeit einzahlt. Beides muss hinreichend gewährleistet werden für einen privatwirtschaftlichen Akteur. Bestehende Zertifizierungsprozesse und anerkannte Rahmenwerke gilt es zu nutzen. Dagegen sieht der Gesetzgeber ein zweistufiges Verfahren vor, bei dem eine technische Prüfung und Zertifizierung kritischer Komponenten mit einer politischen Bewertung der durch die Hersteller abgegebenen Garantieerklärung kombiniert wird. Kritische Komponenten müssen also auf Basis technischer Kriterien geprüft und zertifiziert werden. Zusätzlich dazu müssen die Hersteller von kritischen Komponenten noch eine politische Überprüfung der von ihnen abgegebenen und sich auf die gesamte Lieferkette erstreckenden Garantieerklärung durchlaufen. Letztendlich soll also die Entscheidung darüber, ob eine Kritische Komponente eines bestimmten Herstellers verbaut werden darf oder nicht, auf politischer Ebene getroffen werden.

Ausgehend von der politischen Diskussion, nicht nur eine technische Zertifizierung kritischer Komponenten festzuschreiben, sondern auch die Abgabe von Garantieerklärungen einzufordern, ist es für Bitkom von zentraler Bedeutung, die beiden Säulen auch als solche zu verstehen. § 9 Abs. 4a und die darin beschriebene Entzugsoption von bereits erteilten Zertifikaten durch das BMI ist somit zu streichen. Der Entzug eines erteilten, gültigen technischen Zertifikats ist ausschließlich auf Basis valider (neuer) Erkenntnisse technischer Natur denkbar, nicht aber durch politische Vertraulichkeitsbescheide.

Sofern, trotz erheblicher Bedenken, der Gesetzgeber dennoch an letztgenannten festhalten möchte, so können diese ausschließlich Gegenstand von § 9b sein und bedürfen einer Konkretisierung im Gesetz, um Planungssicherheit und Investitionsschutz sicherzustellen.

Dieser Logik folgend müssen beide Säulen, die technische Zertifizierung Kritischer Komponenten sowie die Abgabe von Garantieerklärungen, nachfolgend losgelöst voneinander adressiert werden:

- **Technische Zertifizierung Kritischer Komponenten**

  Wie bereits erläutert differenziert § 2 Abs. 13 zwischen Kritischen Komponenten, die als kritisch bestimmte Funktionen realisieren und solchen, die gesetzlich bestimmt werden.

  Hinsichtlich der für TK-Diensteanbieter näher spezifizierten Kritischen Komponenten, und wie bereits in der Bitkom Stellungnahmen zum Katalog von Sicherheitsanforderungen gemäß § 109 TKG (§ 162 im Zuge der TKG Novellierung)[1] und zur Liste kritischer Funktionen[2] argumentiert, begrüßen wir grundsätzlich den Ansatz und das Verfahren, Kritische Komponenten über die Umsetzung der kritischen Funktionen zu definieren. Bitkom unterstützt das Bestreben, die kritischen Funktionen eng an der EU-Risikoanalyse und den Implementierungsempfehlungen der EU-Toolbox zu orientieren und technologieneutrale Funktionen für öffentliche Telekommunikationsnetze und -dienste mit erhöhtem Gefährdungspotenzial als Regelungsgegenstand zu beschreiben. Einerseits erscheint dieses Vorgehen zielführender, als eine Gesamtliste kritischer Komponenten zu erarbeiten und fortwährend zu pflegen. Anderseits garantiert eine solche Definition ein angemessenes und schwerlich zu unterlaufendes Verständnis kritischer Komponenten. Allerdings darf es nicht dazu kommen, dass alle der eingesetzten Komponenten als »kritisch« bewertet werden. Dies würde zu einer »Bottom-Up«-Regulierungskette führen, d. h. die über ihre Funktionen als kritisch eingestuften Komponenten würden alle § 9b BSIG-E unterliegen. In Summe können spezifische Komponenten also nur als Ableitung Kritischer Funktionen verstanden werden, wobei auch Funktionen klar zu definieren sind.

  Im Gegensatz dazu lehnt Bitkom die gesetzliche Festlegung Kritischer Komponenten ohne Beteiligung und frühzeitige Einbindung von Unternehmen ab (§ 2 Abs. 13

[1] ↗ Stellungnahme zum Katalog von Sicherheitsanforderungen nach § 109 TKG | Bitkom e.V. sowie Bitkom views concerning the catalogue of security requirements for the operation of telecommunications and data processing systems and for the processing of personal data – pursuant to § 109 of the Telecommunications Act (TKG) Version 2.0 | Bitkom e.V.

[2] ↗ Stellungnahme: zur „Liste der kritischen Funktionen für öffentliche Telekommunikationsnetze und -dienste mit erhöhtem Gefährdungspotenzial“ | Bitkom e.V.

Nr. 1BSIG-E). Betreiber kritischer Infrastrukturen und Hersteller kritischer Komponenten sind vor Bekanntgabe etwaiger Allgemeinverfügungen intensiv zu beteiligen. Bitkom fordert einmal mehr die rechtssichere und hinreichend genaue Definition Kritische Funktionen, um Kritische Komponenten klar fassen/identifizieren zu können. Kritische Komponenten bzw. Komponenten mit kritischen Funktionen können i. S. dieses Gesetzes nur dann kritisch sein, wenn ihre Funktionalitäten in Bezug auf die Einsatzumgebung im Falle ihrer Beeinträchtigung den KRITIS-Schutzzielen zuwiderlaufen. Spezifikationen erfolgen Sektor spezifisch im Rahmen einer Rechtsverordnung unter Beteiligung der betroffenen KRITIS-Sektoren. Grundsätzlich müssen ausreichend lange Umsetzungsfristen gewährt werden. Dies ist insbesondere deshalb wichtig, weil viele Komponenten nicht 1:1 ausgetauscht werden können, sondern weitere Anpassungen erforderlich machen. Es bedarf der Einbindung und Anhörung von Unternehen, bevor eine Komponente gesetzlich als kritisch eingestuft wird. Andernfalls droht Überforderung in Branchen und Unternehmen. Erfahrungswerte aus dem TK-Sektor lassen sich nicht einfach flächendeckend übertragen. Dies verkennt die aktuelle Gesetzesbegründung. Die Zertifizierungspflicht Kritischer Komponenten und die Abgabe von Garantieerklärungen im Sinne des Bestandschutzes können frühestens mit Inkrafttreten des IT-SiG 2.0 erfolgen.

Zusammenfassend festzuhalten ist, dass Bitkom ein hohes Maß an technischer Sicherheit von in Kritischen Infrastrukturen verbauten Komponenten befürwortet und die vorgesehene Säule technischer Zertifizierung auf Basis kritischer Funktionen generell unterstützt. Hersteller wie Betreiber sind dazu bereit, ihre jeweiligen Beiträge zu leisten. Was es braucht, ist allerdings ein klarer, kritikalitätsbasierter Kriterien- und Funktionskatalog, sodass alle Akteure die Sicherheit und Integrität von Komponenten eigenständig verstehen und bewerten können. Bitkom steht bereit, um den weiteren technischen Prozess so praxistauglich und sicherheitssteigernd wie möglich zu gestalten. IT-Sicherheit muss aus technischer Sicht gedacht und adressiert werden. Hierfür ist das BSIG das geeignete Rahmenwerk. Anders sieht es bei der zusätzlichen zweiten Säule aus, der politischen Vertrauenswürdigkeit.

- **Garantieerklärungen und geopolitische Unwägbarkeiten**

Neben der technisch-agnostischen Zertifizierung Kritischer Komponenten wirkt der Begriff der Vertrauenswürdigkeit schwer greifbar. Garantieerklärungen sind ein politisch gewolltes Instrument und bieten keine ausreichende Rechtssicherheit. Objektiv stellt sich für Bitkom die Frage: hilft das gewählte Instrument der Garantieerklärung in seiner jetzigen Ausgestaltung bei der Gewährleistung der Schutzziele? Die Antwort des Bitkom lautet: nein. Die fehlende Benennung konkreter Para-

meter für die Garantieerklärung und der Verweis auf »sicherheitspolitische Belange« führen dazu, dass nach aktueller Lesart bspw. selbst harmlose Wartungsschnittstellen den Entzug der Vertrauenswürdigkeit eines Herstellers rechtfertigen könnten.

Dabei ist sich Bitkom natürlich der geopolitischen Dimensionen und vermeintlichen Beweggründe bewusst. Nicht zuletzt haben wir mit unserem Positionspaper zur Digitalen Souveränität[3] den Diskurs maßgeblich mitgestaltet und unterstützen die EU Toolbox, inkl. der strategischen Maßnahmen. Gleichwohl ist zu konstatieren, dass eindimensionale politische Versuche, die Deutungshoheit rund um Debatten wie 5G, GAIA-X und den Ausschluss von Einzelakteuren zu erlangen, auf den ersten Blick sinnvoll erscheinen mögen. Bei genauerer Betrachtung bringt uns die politische Einordnung der Welt in geopolitische Hemisphären nur bedingt weiter und garantiert uns keineswegs die Fähigkeit, künftig autonom und selbstbestimmt im Sinne unserer Digitalen Souveränität zu handeln.

Im Kern lautet die zentrale Frage: wo soll und wo wird Innovation künftig stattfinden? Innovationen im Digitalkontext werden auch in Zukunft nicht an nationalstaatlichen Grenzen halt machen. Deutsche wie europäischen Entscheidungsträger sollten daher alles daran setzten, unseren digitalen europäischen Binnenmarkt langfristig zu stärken und ein prosperierendes Ökosystem aus nationalen, europäischen und internationalen Playern zu schaffen, die die Innovationen von Morgen in Europa und in Deutschland hervorbringen. Dabei geht es schon längst nicht mehr nur um 5G. Die Wirtschaft ist bereits weiter und beschäftigt sich mit Interoperabilität, OpenRan, Netzwerkvirtualisierung, 6G und vielem mehr – nicht zuletzt, um aus privatwirtschaftlichen Gründen einseitige Abhängigkeiten zu reduzieren und neue Handlungsalternativen aus eigenen Stücken heraus zu schaffen. Bitkom wünscht sich einen grundsätzlichen Narrativwechsel, im Sinne einer proaktiven, bestmöglichen Unterstützung und Förderung des von der Wirtschaft bereits eingeschlagenen Wegs. Zur Stärkung der europäischen und deutschen Wirtschaft braucht es dazu eine ressortübergreifend kooperativ-ausgerichtete, zukunfts- und europäisch-fokussierte sowie sicherheits- und forschungsgetriebene Innovations- und Industriepolitik.

Als Digitalwirtschaft sind wir uns unserer Rolle im IT-Sicherheitskontext bewusst und alle Einzelakteure zur Mitwirkung im Rahmen der individuellen Möglichkeiten bereit, den Schutze nationaler und europäischer Kritischer Infrastrukturen mitzugestalten. Mit dem Vorhaben, politisch die Oberhand und das Letztentscheidungsrecht behalten zu wollen – entgegen aller Unwägbarkeiten und negativen Auswirkun-

[3] ↗ Digitale Souveränität: Anforderungen an Technologien- und Kompetenzfelder mit Schlüsselfunktion | Bitkom e.V.

gen auf wirtschaftliche Prozesse und Innovationen – liegt der Ball allerdings weit im Feld der nationalen Politik. Sie muss sich daran messen lassen.

- **Zentrale Aspekte, die es bei der Vertrauenswürdigkeitsprüfung hervorzuheben gilt**

  - Grundsätzlich gilt, dass der Entzug der Vertrauenswürdigkeit und etwaige damit verbundene Rückbauverpflichtungen ein enormes Investitionsrisiko darstellen und im Extremfall die Existenz eines Unternehmens gefährden. Es gibt weder eine Haftungsdeckelung noch eine Haftungszuweisung. Wenngleich Bitkom bereits die jetzige Ausgestaltung der Vertrauenswürdigkeitsprüfung nicht unterstützt, muss explizit auf nachgelagerte Unwägbarkeiten und Risiken hingewiesen werden. Was soll geschehen, wenn ein Lieferant seine Vertrauenswürdigkeit einbüßt, obgleich bereits seine Technik Bestandteil der Infrastruktur ist? Der Gesetzesentwurf nennt den Rückbau von verbauten Komponenten explizit als Option. Dies ist im Sinne des Bestandsschutzes nicht tragbar und daher abzulehnen. Klare Verantwortlichkeiten, Ausstiegsszenarien und Übergangsfristen müssen Rechtssicherheit garantieren. Nach aktuellem Stand des Gesetzestextes drohen bspw. der europäischen Mobilfunkbranche Mehrkosten von mehreren Milliarden Euro, wodurch Verzögerungen im (5G-)Netzausbau nicht ausgeschlossen werden können. Falls der Gesetzgeber tatsächlich am Vorhaben festhalten sollte, ist ein ausreichend ausgestatteter Kompensationsfonds zu schaffen. Andernfalls werden die mittelfristig anfallenden Kosten eines international nicht kompetitiven Telekommunikationsnetzes für Wirtschaft, Wissenschaft, Gesellschaft und Politik um ein vielfaches höher ausfallen und Deutschland als Zukunftsstandort von Schlüsselindustrien international zurückwerfen.

  - Um die Beschaffungspflichten und damit die Ausstattungsfähigkeiten der Betreiber kritischer Infrastrukturen realistisch abzubilden, bedarf es der Klarstellung/ Anerkennung, dass Betreiber Kritischer Infrastrukturen die Hoheit über und auch die Verantwortung für ihre Prozesse, Ausstattungen und Geschäftstätigkeit haben. Somit obliegt ihnen die Einschätzung der entsprechenden Kritikalität im Gesamtkontext. Diese Kompetenzen können weder vom BSI abgebildet werden, noch erscheint es als sinnvoll, die Verantwortung auf die Hersteller zu projizieren. Gleichwohl müssen natürlich auch die Hersteller in die Pflicht genommen werden und ihren Beitrag zur Erhöhung der Sicherheit informationstechnischer Systeme leisten. Eine Blankogarantie über die Vertrauenswürdigkeit der gesamten Lieferketten gemäß § 9b Abs. 2 Satz 2 BSIG-E gehört aber nicht dazu und ist nicht praktikabel. Es sollte explizit auf bestehende und international anerkannte Zertifizierungsrahmen verwiesen werden, um den zu erwartenden Bürokratieaufwand

so gering wie möglich zu halten. Es ist überlegenswert, ob nicht Akteure, die schon heute im Rahmen von KRITIS, der TKG oder anderen gesetzlichen Verpflichtungen, einer herausgehobenen Nachweispflicht nachkommen müssen, von einer weiteren (zweiten) Nachweisplicht ausgenommen werden sollten, sodass eine objektiv unnötige Doppelpflicht und -aufsicht ausgeschlossen ist.

- Ferner muss verhindert werden, dass durch vorsätzlich begangene und schuldhaft herbeigeführte unerlaubte Handlungen eines Herstellers den Betreibern gesetzlich nicht abgedeckte finanzielle Schäden entstehen. In gleicher Manier ist es zu vermeiden, dass sich Hersteller von Kritischen Komponenten in Rechtsstreitigkeiten wiederfinden, wo sie sich über Jahre hinweg gegen schwer nachweisbare Anschuldigungen und politisch gewollte Entscheidungen zur Wehr setzen mussten. Sollte es jedoch zum Entzug der Vertrauenswürdigkeit eines Herstellers kommen, darf dies nur Folgen für Kritische Komponenten des Herstellers haben, nicht aber für nicht-Kritische Komponenten. Die Formulierung in § 9b Abs. 6 ist daher zu begrüßen.

- Abschließend ist explizit zu betonen, dass die Zertifizierungspflicht Kritischer Komponenten und die Abgabe von Garantieerklärungen frühestens mit Inkrafttreten des IT-SiG 2.0 erfolgen kann. Erfahrungsgemäß ist davon auszugehen, dass eine mehrjährige Übergangfrist nach Inkrafttreten nötig sein wird, alleine um die Zertifizierungsprozesse durchlaufen zu können.

Ermächtigung zum Erlass von Rechtsverordnungen

Der in § 10 Abs. 6. enthaltene Ansatz, Interoperabilität erstmalig explizit als eine gestalterische Maßnahme mit Visionspotenzial zur langfristigen Steigerung der IT-Sicherheit im Gesetzestext zu nennen, ist positiv zu würdigen. In Ermangelung einer Gesetzesbegründung – inkl. europarechtlicher Einordnung – und der damit fehlenden Möglichkeit der abschließenden Bewertung, wird dieser Absatz in der Branche kontrovers diskutiert. Eine intensive Einbeziehung der betroffenen Sektoren ist nicht nur im Zuge der Veröffentlichung einer etwaigen Rechtsverordnung erforderlich, sondern auch schon bei der weiteren Ausgestaltung des Gesetzgebungsprozesses.

Bußgelder

Es bedarf einer Balance zwischen maßvoller und wirksamer Sanktionierung. Die aktuell festgeschriebenen Bußgeldhöhen für Ordnungswidrigkeiten erachtet Bitkom mit Blick auf den Geltungsbereich des IT-SiG 2.0 als nachvollziehbar. Allerdings darf es für

Bitkom keinen Verweis auf § 30 Abs.2 Satz 3 OWiG und die damit verbundene Möglichkeit hebelbarer Bußgelder geben. Andernfalls müssten Unternehmen die gesamte Fülle der nachfolgend gelisteten, hebelbaren Ordnungswidrigkeiten fürchten und enorme Summen an Rückstellungen bilden, die dann wiederum nicht in risikobasiert identifizierte Schutzmaßnahmen zur Absicherung der Infrastrukturen investiert werden könnten. Im EU-Durchschnitt ist die Höhe der Bußgelder zudem um ein vielfaches geringer und es erschließt sich nicht, weshalb Unternehmen in Deutschland wettbewerblich benachteiligt werden sollten.

Es darf nicht übersehen werden, dass die Erhöhung der IT-Sicherheit ein wesentliches unternehmerisches Interesse der Verpflichteten darstellt. Dies gilt insbesondere hinsichtlich der bestehenden vertraglichen und außervertraglichen Pflichten gegenüber Kunden, der Wettbewerbssituation im Markt sowie der Verantwortung von Unternehmen gegenüber Aktionären und Investoren.

Bitkom vertritt mehr als 2.700 Unternehmen der digitalen Wirtschaft, davon gut 2.000 Direktmitglieder. Sie erzielen allein mit IT- und Telekommunikationsleistungen jährlich Umsätze von 190 Milliarden Euro, darunter Exporte in Höhe von 50 Milliarden Euro. Die Bitkom-Mitglieder beschäftigen in Deutschland mehr als 2 Millionen Mitarbeiterinnen und Mitarbeiter. Zu den Mitgliedern zählen mehr als 1.000 Mittelständler, über 500 Startups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Geräte und Bauteile her, sind im Bereich der digitalen Medien tätig oder in anderer Weise Teil der digitalen Wirtschaft. 80 Prozent der Unternehmen haben ihren Hauptsitz in Deutschland, jeweils 8 Prozent kommen aus Europa und den USA, 4 Prozent aus anderen Regionen. Bitkom fördert und treibt die digitale Transformation der deutschen Wirtschaft und setzt sich für eine breite gesellschaftliche Teilhabe an den digitalen Entwicklungen ein. Ziel ist es, Deutschland zu einem weltweit führenden Digitalstandort zu machen.

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
19(4)741 B

Stiftung Neue Verantwortung

Sachverständigenstellungnahme von Dr. Sven Herpig[1], Leiter für Internationale Cybersicherheitspolitik bei der Stiftung Neue Verantwortung e. V., für die Sitzung des Bundestagsausschusses für Inneres und Heimat am 01.03.2021 zum Entwurf eines Zweiten Gesetzes zur Erhöhung der Sicherheit Informationstechnischer Systeme – BT-Drucksache 19/26106

Der Sachverständige bedankt sich bei Jan-Peter Kleinhans[2] für seinen Beitrag zu § 9b BSIG-E in Verbindung mit § 2 Absatz 13 BSIG-E „Kritische Komponenten und vertrauenswürdige Hersteller“.

Der Sachverständige bedankt sich bei diversen Expert:innen der deutschen Cybersicherheitspolitik für die Unterstützung.

Kontakt

Dr. Sven Herpig
sherpig@stiftung-nv.de
@z_edian (Twitter)
Stiftung Neue Verantwortung

[1] Stiftung Neue Verantwortung (2021): Experten-Profil „Dr. Sven Herpig“
[2] Stiftung Neue Verantwortung (2021): Experten-Profil „Jan-Peter Kleinhans“

Stiftung Neue Verantwortung

A. Gesamtkritik

Im Vergleich zum Referentenentwurf vom 27. März 2019[3] ist bei der vorliegenden Fassung vom 25. Januar 2021 zu begrüßen, dass die Änderungen zum StGB und StPO – und hier im Besonderen § 126a StGB, § 202e StGB, § 202f StGB und § 163g StPO – wie in der vorläufigen Bewertung vom 8. Mai 2019 angeregt[4], ersatzlos gestrichen worden sind. Nach gesicherten rechtswissenschaftlichen Erkenntnissen ist eine Verschärfung des Strafrechts kein geeignetes bzw. effektives Mittel zur Reduktion von Straftaten[5] und hätte in diesem Kontext daher auch nicht zu mehr IT-Sicherheit beigetragen.

Im Vergleich zum Referentenentwurf vom 7. Mai 2020[6] ist bei der vorliegenden Fassung vom 25. Januar 2021 zu begrüßen, dass durch Auslassung des Begriffs „Infrastruktur im besonderen öffentlichen Interesse" mehr Klarheit bei der Terminologie geschaffen wurde (vgl. *4. Unternehmen im besonderen öffentlichen Interesse*), wie in der vorläufigen Bewertung vom 9. Juni 2020 angeregt. Weiterhin ist zu begrüßen, dass – wie auch in der vorläufigen Bewertung angeregt – die Norm § 7a BSIG-E Absatz 1 Satz 2 auf Nummern 1, 14, 14a, 17 und 18 verengt wurde (vgl. *6. Untersuchung der Sicherheit in der Informationstechnik*).

Im Vergleich zum Referentenentwurf vom 1. Dezember 2020[7] ist bei der vorliegenden Fassung vom 25. Januar 2021 zu begrüßen, dass die Änderungen der Norm § 15 TMG ersatzlos gestrichen worden sind. Weiterhin ist zu begrüßen, dass, wie u. a. in den vorläufigen Bewertungen vom 9. Juni und 1. Dezember 2020 angeregt, die Evaluation der Effektivität dieser Gesetzesänderungen untersucht werden muss (vgl. „zu Artikel 6 (Evaluierung)") um Anpassungsbedarf zu ermitteln.

Vor der Analyse spezifischer Einzelpunkte des Gesetzesentwurfs wird übergeordnet angeregt, dass sich der Bundestag in seiner Befassung allen Normen des vorliegenden Gesetzestextes widmet und nicht ausschließlich der Vertrauenswürdigkeitserklärung für Hersteller kritischer Komponenten u. a. § 9b BSIG-E („5G-Debatte").

Diese Analyse des Gesetzesentwurfs mit angeschlossenen Empfehlungen befasst sich mit den folgenden Einzelpunkten:

1. IT-Sicherheit für die Gesellschaft durch Verbraucherschutz
2. Evaluierung der bisherigen IT- und Cybersicherheitsmaßnahmen
3. Mobile Incident Response Teams
4. Unternehmen im besonderen öffentlichen Interesse und Parteien
5. Schwachstellenmanagement und -meldewesen
6. Untersuchung der Sicherheit in der Informationstechnik
7. IT-Sicherheit in Digitalisierungsvorhaben
8. Kritische Komponenten und vertrauenswürdige Hersteller

[3] Andre Meister und Anna Biselli (2019): T-Sicherheitsgesetz 2.0: Wir veröffentlichen den Entwurf, der das BSI zur Hackerbehörde machen soll
[4] Sven Herpig (2019): Vorläufige Bewertung des Referentenentwurfs zum IT-Sicherheitsgesetz 2.0
[5] Siehe u. a. Wolfgang Heinz (2007): Mehr und härtere Strafen = mehr Innere Sicherheit! Stimmt diese Gleichung? Strafrechtspolitik und Sanktionierungspraxis in Deutschland im Lichte kriminologischer Forschung
[6] Andre Meister (2020): Seehofer will BSI zur Hackerbehörde ausbauen
[7] Bundesministerium des Innern, für Bau und Heimat (2020): Referentenentwurf des Bundesministeriums des Innern, für Bau und Heimat Entwurf eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme

9. Eingriff der Diensteanbieter in die Integrität von Kundensystemen
10. Anordnungsbefugnis gegenüber Diensteanbietern
11. Sonderrolle von Auswärtigem Amt und Bundeswehr und Mindeststandards nur im Einvernehmen
12. Staatliche Cybersicherheitsarchitektur

Allgemein ist zu kritisieren, dass die Aktualisierung des Gesetzes ohne eine Evaluierung des vorangegangenen ersten IT-Sicherheitsgesetzes geplant wird, vor allem da ohne jegliche Evidenz von „Erfahrungen mit der Anwendung der im ersten IT-Sicherheitsgesetz geregelten Befugnisse“ (s. A. Allgemeiner Teil, II. Wesentlicher Inhalt des Entwurfs) gesprochen wird. Bereits bei dem Entwurf der Cybersicherheitsstrategie für Deutschland 2016 gab es keine Evaluierung der Cybersicherheitsstrategie 2011. Dieses Versäumnis wiegt in dem vorliegenden Vorhaben zum IT-Sicherheitsgesetz 2.0 noch weitaus schwerer, da im Vorgängergesetz sogar eine Teilevaluierung rechtlich verankert wurde.[8] Die Evaluierung von Maßnahmen ist ein elementarer Bestandteil staatlichen Handelns und sollte auch bei diesem Gesetzgebungsvorhaben durchgeführt werden, bevor eine Kompetenz- und Anforderungsausweitung verabschiedet wird. Offensichtlich wird im Bereich der IT- und Cybersicherheitspolitik weiterhin versucht, sicherheitsbehördliche Kompetenzen auszubauen, ohne die Effektivität existierender Kompetenzen vorher zu evaluieren.

Der aktuelle Gesetzesentwurf ignoriert weiterhin die im Koalitionsvertrag[9] festgelegte "gleichzeitige und entsprechende Ausweitung der parlamentarischen Kontrolle" bei Ausweitung der Befugnisse der Sicherheitsbehörden. Das ist höchst problematisch, da die Bundesregierung bislang noch immer nicht die vom Bundesverfassungsgericht 2010 angeregte Gesamtschau der staatlichen Überwachungsmaßnahmen ("Überwachungsgesamtrechnung")[10] vorgelegt hat. Eine Befugnis-Erweiterung der Sicherheitsbehörden im IT-Sicherheitsgesetz 2.0 sollte unbedingt durch geeignete und angemessene Schutzmechanismen und Kontrollmaßnahmen begrenzt werden.

Auch auf die im Koalitionsvertrag vereinbarte Stärkung des Bundesamts für Sicherheit in der Informationstechnik "in seiner Rolle als unabhängige und neutrale Beratungsstelle für Fragen der IT-Sicherheit"[11] wird in dem Entwurf nicht eingegangen. Der Entwurf sollte zumindest eine Prüfung unterschiedlicher Unabhängigkeitsmodelle vorsehen.[12]

Zu dem Mangel empirischer Evidenz bei der Normengestaltung[13] und fehlender Berücksichtigung der Vorgaben aus dem Koalitionsvertrag kommen weitere Defizite, auf die im Folgenden eingegangen wird. Eine weitere Überarbeitung des Entwurfs wäre daher zielführend, um die Cyber- und Informationssicherheit in Deutschland nachhaltig zu stärken.

[8] Bundesanzeiger (2015): Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz)
[9] Bundesregierung (2018): Koalitionsvertrag zwischen CDU, CSU und SPD
[10] digitalcourage (2021): Überwachungsgesamtrechnung
[11] Bundesregierung (2018): Koalitionsvertrag zwischen CDU, CSU und SPD
[12] Sven Herpig (2020): Die "Unabhängigkeit" des Bundesamtes für Sicherheit in der Informationstechnik
[13] Sven Herpig (2019): Sachverständigenstellungnahme im Ausschuss des Deutschen Bundestags für Inneres und Heimat

Weiterhin wird darauf hingewiesen, dass das Bundesministerium des Innern, für Bau und Heimat bei der „Vorbereitung dieses Regelungsvorhabens in mehrfacher Hinsicht gegen die Grundsätze Besserer Rechtsetzung verstoßen [hat]“.[14]

[14] Deutscher Bundestag (2021), Gesetzentwurf der Bundesregierung, Entwurf eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme – Anlage 2: Stellungnahme des Nationalen Normenkontrollrates gem. § 6 Absatz 1 NKRG und Sven Herpig (2021): Policy-Making in Deutschland am Beispiel des IT-Sicherheitsgesetzes 2.0 – ein Twitter Thread

B. Einzelkritik

1. IT-Sicherheit für die Gesellschaft durch Verbraucherschutz

A. „Problem und Ziel“ in Verbindung mit „B. Lösung“ und Verweis auf §§ 3 und 9c BSIG-E

Der Entwurf definiert den Schutz von Gesellschaft als eines der Kernziele des Gesetzes. Als Hauptmaßnahme zum Schutz der Bürger:innen, und der damit verbundenen größten Personalaufwendung, führt der Entwurf die Einführung des „IT-Sicherheitskennzeichens“ an. Allerdings wird das IT-Sicherheitskennzeichen nicht direkt zu einer Erhöhung der IT- und Cybersicherheit in Deutschland führen. Eine indirekte Erhöhung der IT- und Cybersicherheit wäre bei verpflichtenden IT-Sicherheitssiegeln zumindest durch die Beeinflussung der Kaufentscheidung und des damit einhergehenden Einflusses auf Hersteller, die sich um eine verbesserte IT-Sicherheit ihrer Produkte bemühen müssten, gegeben.[15] Wenn eine Kennzeichnung mit dem IT-Sicherheitskennzeichen in Verbindung mit dem elektronischen Beipackzettel freiwillig ist, signalisiert es nur, wie (un)sicher ein Produkt ist. Weder die Produkte noch die Bürger:innen/Gesellschaft werden damit direkt sicherer. Zugespitzt bedeutet dies, dass IT-Produkte, deren Schutzmechanismen im Entwurf selbst als „faktisch wirkungslos“ bezeichnet werden, weiterhin verkauft werden dürften und nur auf Basis von Freiwilligkeit des Herstellers ein entsprechendes IT-(Un)Sicherheitskennzeichen auf der Verpackung tragen würden. Gleichzeitig entsteht durch die in §§ 9c und 3 Absatz 14 BSIG-E erwähnten Aufgaben ein hoher Mehraufwand für das Bundesamt für Sicherheit in der Informationstechnik. Es ist zu bezweifeln, dass der Ertrag den Aufwand beim freiwilligen IT-Sicherheitskennzeichen rechtfertigt. Die Maßnahme ist möglicherweise effektiv, aber keineswegs effizient. Vor dem Hintergrund der nach wie vor herrschenden Knappheit an IT-Sicherheitsfachkräften im öffentlichen Dienst sollte diese Maßnahme dringend überdacht werden.

Empfehlung: Die Bundesregierung sollte darauf hinarbeiten, dass bekanntermaßen unsichere und nicht mehr absicherbare IT-Produkte überhaupt nicht in den Handel gelangen dürfen.[16] Weiterhin sollten konkrete Maßnahmen ergriffen werden, die direkt für eine höhere Sicherheit der Bürger:innen sorgen, wie z. B. eine voreingestellte Netzwerksegmentierung bei Routern (Heimnetz/ IoT-Geräte). Die Idee des IT-Sicherheitskennzeichens sollte stattdessen direkt auf EU-Ebene angegangen werden, damit der Einsatz von verpflichtenden statt nur freiwilligen Siegeln ermöglicht werden kann (siehe „Warenverkehrsfreiheit“). Gleichzeitig muss sichergestellt werden, dass ein (freiwilliges) IT-Sicherheitskennzeichen nicht mit höherwertigen Zertifizierungen von Produkten vermischt wird.

[15] Philipp Morgner, Christoph Mai, Nicole Koschate-Fischer, Felix Freiling und Zinaida Benenson (2019): Security Update Labels: Establishing Economic Incentives for Security Patching of IoT Consumer Products
[16] Verbraucherzentrale Nordrhein-Westfalen (2020): Vorerst keine Sicherheit für Handynutzer: Urteil Oberlandesgericht Köln

2. Evaluierung der bisherigen IT- und Cybersicherheitsmaßnahmen

„A. Problem und Ziel“ in Verbindung mit „C. Alternativen“

Als sehr weit gefasste Zielvorgabe gibt der Entwurf vor, dass „die Gewährleistung der Cyber- und Informationssicherheit [ein] Schlüsselthema für Staat, Wirtschaft und Gesellschaft [ist]“. Eine Alternative zu allen im Entwurf vorgeschlagenen Normen wird nicht genannt. Es ist schwer nachvollziehbar, dass bei einer so umfassenden Zielvorgabe keine einzige Alternative genannt werden kann. Dies ist möglicherweise auf die fehlende Evaluierung der Effektivität der bisher implementierten staatlichen Maßnahmen zur Erhöhung der Cyber- und IT-Sicherheit in Deutschland zurückzuführen.

Empfehlung: Die Bundesregierung sollte die Effektivität der bisher getroffen Cyber- und IT-Sicherheitsmaßnahmen evaluieren und unter Einbeziehung der Expertise aus Wirtschaft, Wissenschaft und Zivilgesellschaft Alternativen entwerfen, bevor der vorliegende Gesetzestext als alternativlos bezeichnet wird.

3. Mobile Incident Response Teams

„E.3 Erfüllungsaufwand der Verwaltung“ in Verbindung mit § 5b BSIG-E

Die Mobile Incident Response Teams (MIRTs) des Bundesamtes für Sicherheit in der Informationstechnik sind ein Kernelement reaktiver Maßnahmen in der deutschen Cyber- und IT-Sicherheitspolitik. Der Mehrwert der MIRTs für die deutsche Cyber- und IT-Sicherheitspolitik ist für die Öffentlichkeit nachvollziehbar, wie u. a. der Fall des Lukaskrankenhauses in Neuss[17] gezeigt hat.

Empfehlung: Ein Ausbau der MIRTs ist zu unterstützen, da für diese eine breite Fachexpertise – zum Beispiel für die unterschiedlichen Systeme Kritischer Infrastrukturen – bereitgehalten werden muss. Der genannte Ausbau der Teams wäre eine effiziente Investition der im Entwurf insgesamt vorgesehenen Personalressourcen. Es ist dabei jedoch unklar, wie viele MIRTs notwendig sind, u. a. wegen Bereitschaftszeiten und Spezialexpertise. Es sollte daher dargelegt werden, welcher Plan hinter dem Ausbau der MIRTs steht und wie viele dieser Teams zu welchem Zeitpunkt für welche Einsatzgebiete (Regierung, KRITIS o. ä.) bereitstehen müssen. Dieser Plan sollte auch Transparenz über Einsatzstatus, Aufgabenteilung und Einsatzgebiete der „Quick Reaction Forces“ des Bundeskriminalamts, der „Mobile Cyber-Teams“ des Bundesamts für Verfassungsschutz und analoger Teams des Militärischen Abschirmdiensts und Bundesnachrichtendiensts herstellen.[18] Zudem sollte eine Einbettung des Konzepts des Cyber-Hilfswerks[19] in diesen Plan geprüft werden.

[17] Noah Gottschalk (2017): Wenn eine Klinik ohne Computer arbeiten muss
[18] Bundesministerium des Innern (2016): Cyber-Sicherheitsstrategie für Deutschland 2016
[19] AG KRITIS (2020): Cyber-Hilfswerk (CHW)

4. Unternehmen im besonderen öffentlichen Interesse und Parteien

§ 2 Absatz 14 BSIG-E in Verbindung mit §§ 2 Absatz 3 Satz 2, 8, 8f und 10 Absatz 5 BSIG-E

Es ist unklar, in welchem Verhältnis die bestehenden „Institutionen im besonderen staatlichen Interesse" (INSI)[20] zu den im Entwurf erstmals erwähnten „Unternehmen im besonderen öffentlichen Interesse" gem. § 8f BSIG-E und der „Infrastruktur im besonderen öffentlichen Interesse“ gem. § 109a Abs 8 TKG-E stehen. Weder in der aktuellen EU NIS-Richtlinie[21] noch in dem entsprechenden Umsetzungsgesetz[22] finden sich diese Begrifflichkeiten wieder. Im Umsetzungsgesetz wird lediglich einmal von „informationstechnischen Systemen von besonderem öffentlichem Interesse" gesprochen (§ 5a Absatz 2 BSIG). Diese Inkonsistenzen wirken einer Harmonisierung entgegen und verstärken die Komplexität durch die unilaterale Einführung einer weiteren „Schutzklasse“.

Empfehlung: Die Bundesregierung muss Transparenz bzgl. der „Institutionen im besonderen staatlichen Interesse“ im Vergleich zu „Unternehmen im besonderen öffentlichen Interesse“ schaffen. Gleichzeitig sollten die Kategorien der deutschen Gesetzgebung nicht von der EU-Harmonisierung abweichen, weshalb eine zusätzliche, unilaterale Einführung der „Unternehmen im besonderen öffentlichen Interesse“ o. ä. verworfen werden sollte – bis es entsprechende Vorgaben auf EU-Ebene gibt, z. B. durch eine verabschiedete NIS II[23]. Auch inhaltlich erscheint diese zusätzliche Kategorie nicht sinnvoll: Entweder werden Unternehmen als kritisch genug betrachtet, um sie bzgl. IT-Sicherheit zu regulieren und folglich unter der KRITIS-Regulierung zu subsumieren, oder aber sie werden als nicht relevant genug eingeordnet, um bzgl. IT-Sicherheit reguliert zu werden. In diesem Fall können sie dann unter den bestehenden, unbestimmten Rechtsbegriff der „Institutionen im besonderen staatlichen Interesse“ fallen. Eine Ausdifferenzierung kann bei Aufnahme in die KRITIS-Regulierung über die branchenspezifischen Sicherheitsstandards[24] stattfinden.

Darüber hinaus ist zu prüfen, ob politische Parteien ab einer bestimmten Mitgliederanzahl wegen ihrer Relevanz für das Funktionieren des deutschen Staates in die KRITIS-Regulierung aufgenommen werden sollten.[25] Vor dem Hintergrund der Gewaltenteilung könnten alternativ Mindeststandards für die Sicherheit der Informationstechnik des Bundes gem. § 8 für Parteien empfehlenden Charakter haben, analog zu der Regelung für Gerichte und Verfassungsorgane nach § 2 Absatz 3 Satz 2.

Sollte die Bundesregierung an der Einführung der zusätzlichen Kategorie „Unternehmen im besonderen öffentlichen Interesse“ festhalten, so ist zumindest § 10 Absatz 5 BSIG-E um die Beteiligung der organisierten Zivilgesellschaft zu erweitern.

[20] Bundesamt für Sicherheit in der Informationstechnik (2021): Allianz für Cyber-Sicherheit Teilnehmer werden
[21] Amtsblatt der Europäischen Union (2016): RICHTLINIE (EU) 2016/1148 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 6. Juli 2016
[22] Bundesgesetzblatt (2016): Gesetz zur Umsetzung der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016
[23] European Commission (2020): Proposal for directive on measures for high common level of cybersecurity across the Union
[24] Bundesamt für Sicherheit in der Informationstechnik (2021): Branchenspezifischer Sicherheitsstandard
[25] Sven Herpig und Julia Schuetze (2019): Mehr IT-Sicherheit für deutsche Wahlen

Stiftung
Neue
Verantwortung

5. Schwachstellenmanagement und -meldewesen

§ 4b BSIG-E in Verbindung mit §§ 7, 7a, 7b und 7c BSIG-E

Der Umgang mit Schwachstellen ist ein elementarer Aspekt zur Herstellung von IT-Sicherheit in Unternehmen und Behörden. Klare Prozesse und Verantwortlichkeiten, die der technischen Komplexität Rechnung tragen, sind daher unbedingt notwendig. Die mit dem Entwurf geplante Regulierung bzgl. des staatlichen Schwachstellenmanagements und -meldewesens ist intransparent. Es ist zu erwarten, dass diese Intransparenz zu ineffektiven Prozessen und einem Vertrauensverlust bei Firmen und IT-Sicherheitsforscher:innen – Akteuren, die wichtig für den Erfolg einer solchen Policy sind – führen wird.

Empfehlung: Empfohlen wird ein Verweis auf eine separate Verordnung o. ä., die den Umgang mit Schwachstellen durch Behörden dezidiert regelt, anstatt einer Regelung der Prozesse über die im Entwurf angeführten Normen. Zudem wird eine Einführung des seit Jahren in Planung befindlichen Schwachstellenmanagements des Bundesministeriums des Innern, für Bau und Heimat am Beispiel des von der Stiftung Neue Verantwortung vorgelegten Entwurfs empfohlen[26]. Gleichzeitig sollte ein Errichtungsgesetz für die Schwachstellen-verarbeitende Zentrale Stelle für Informationstechnik im Sicherheitsbereich erarbeitet werden. Das ist dringend notwendig, da die Behörde ihre invasive Tätigkeit momentan ohne eine solche Gesetzesgrundlage ausübt. In den Gesetzen aller Schwachstellen-verarbeitenden Sicherheitsbehörden auf Bundesebene (u. a. Bundesnachrichtendienst, Bundeskriminalamt, Bundespolizei, Bundesamt für Verfassungsschutz, Bundeswehr, Zentrale Stelle für Informationstechnik im Sicherheitsbereich) muss eine Reziprozität bzgl. der Weitergabe von Schwachstellen ergänzt werden: Während das Bundesamt für Sicherheit in der Informationstechnik gem. § 3 Absatz 1 Satz 13 BSIG andere Bundesbehörden bei der Wahrnehmung ihrer gesetzlichen Aufgaben unterstützen muss, sind diese Bundesbehörden ihrerseits nicht verpflichtet, das Bundesamt für Sicherheit in der Informationstechnik durch die Weitergabe der von ihnen gefundenen oder erworbenen Schwachstellen zu unterstützen. Dies ist allerdings eine Grundvoraussetzung für die Wahrnehmung der gesetzlichen Aufgaben des Bundesamtes für Sicherheit in der Informationstechnik.

Auch vor diesem Hintergrund wäre eine stärkere fachliche Unabhängigkeit des Bundesamtes für Sicherheit in der Informationstechnik vom Bundesministerium des Innern, für Bau und Heimat zielführend.

[26] Sven Herpig (2018): Schwachstellen-Management für mehr Sicherheit

6. Untersuchung der Sicherheit in der Informationstechnik

§ 7a BSIG-E in Verbindung mit §§ 7, 7a, 7b und 7c BSIG-E

Die Norm enthält wenige Einschränkungen darüber, welche informationstechnischen Produkte und Systeme das Bundesamt für Sicherheit in der Informationstechnik untersuchen darf (Absatz 1). Darüber hinaus darf das Bundesamt für Sicherheit in der Informationstechnik in diesem Kontext alle notwendigen Informationen von den Herstellern einfordern (Absatz 2). Eine anlasslose Untersuchung aller informationstechnischen Produkte und Systeme mit einer zusätzlichen Befugnis, externe Informationen anzufordern, ist sehr breit. Gleichzeitig werden dem Bundesamt kaum Beschränkungen auferlegt, wie es mit den so erworbenen Informationen verfahren darf (Verweis auf die sehr breite Norm § 3 Absatz 1 Satz 2 BSIG). Dies könnte folglich auch die Weitergabe von Informationen zu Schwachstellen an andere Sicherheitsbehörden beinhalten, welche die Schwachstellen ausnutzen und damit dem gesetzlichen Auftrag des Bundesamtes für Sicherheit in der Informationstechnik zuwiderhandeln würden.

Empfehlung: Zusätzlich zu den unter „5. Schwachstellenmanagement und -meldewesen“ genannten Empfehlungen sollte aufgrund der vorausgegangenen Analyse eine defensive Zweckbindung der so erlangten Informationen über die IT-Produkte und Systeme eingefügt werden (Absätze 2, 3 und 4). Zusätzlich sollte eine weitere Verengung der Norm geprüft werden.

7. IT-Sicherheit in Digitalisierungsvorhaben

§ 8 Absatz 4 BSIG-E

Die Zeitangabe “frühzeitig” im Kontext der Einbindung des Bundesamtes für Sicherheit in der Informationstechnik in Digitalisierungsvorhaben des Bundes wird in dieser Norm nicht näher definiert. Zusätzlich ist das Bundesamt für Sicherheit in der Informationstechnik gegenüber dem Bundesministerium des Innern, für Bau und Heimat fachlich weisungsgebunden und das Ministerium muss über jede Zusammenarbeit des Bundesamts für Sicherheit in der Informationstechnik informiert werden (vgl. § 26 GGO). Vor dem Hintergrund dieser Beschränkungen führt die Norm wahrscheinlich nicht zu der beabsichtigten früheren Einbindung des Bundesamts für Sicherheit in der Informationstechnik in Digitalisierungsvorhaben der Bundesverwaltung.

Empfehlung: Die Angabe „frühzeitig“ sollte präzisiert bzw. ein grober Zeitraum inkludiert werden. Weiterhin sollte ermöglicht werden, dass andere Behörden die Unterstützung des Bundesamts für Sicherheit in der Informationstechnik direkt und ohne vorherigen Kontakt zum Bundesministerium des Innern, für Bau und Heimat ersuchen können. Das würde auch die im Koalitionsvertrag angekündigte Stärkung des Bundesamts für Sicherheit in der Informationstechnik "in seiner Rolle als unabhängige und neutrale Beratungsstelle für Fragen der IT-Sicherheit"[27] fördern.

[27] Bundesregierung (2018): Koalitionsvertrag zwischen CDU, CSU und SPD

8. Kritische Komponenten und vertrauenswürdige Hersteller

§ 9b BSIG-E in Verbindung mit § 2 Absatz 13 BSIG-E

Die sehr breite Definition von „kritischen Komponenten“ in Verbindung mit der Garantieerklärung über die „gesamte Lieferkette des Herstellers“ auf Basis einer nicht näher definierten späteren Allgemeinverfügung des Bundesministeriums des Innern, für Bau und Heimat macht eine Bewertung dieser Norm ohne weitere Details schwer möglich. Der Anwendungsbereich dieser Norm geht weit über die technische IT- und Cybersicherheit hinaus, für die das Bundesamt für Sicherheit in der Informationstechnik – und damit das BSIG – verantwortlich ist. Dies wird unter anderem dadurch deutlich, dass in diesem Kontext das Bundesministerium des Innern, für Bau und Heimat und nicht mehr das Bundesamt für Sicherheit in der Informationstechnik genannt wird. Diese Perspektive wird dadurch verstärkt, dass sowohl die Inhalte der Garantieerklärung als auch die Risikobewertung des Herstellers der kritischen Komponente „im Einvernehmen mit den jeweils betroffenen Ressorts erfolgen“. Weiterhin soll zur Unterstützung ein fortlaufender Austausch durch einen „interministeriellen Jour Fixe […] (BMI, BMWi, AA, Bundeskanzleramt auf Ebene Referatsleitung)“ sichergestellt werden. Die Grundlage für eine fortlaufende, interministerielle Bewertung des Risikoprofils eines Herstellers, u. a. hinsichtlich „Organisationsstruktur […] Handlungen […] rechtlichen Verpflichtungen“ sollte jedoch nicht im BSIG-E gelegt werden. Gleichzeitig ist eine solche interministerielle Bewertung unter Einbeziehung sicherheitspolitischer Belange essenziell.

Hinsichtlich zukünftiger Telekommunikationsnetze muss auch grundsätzlich in Frage gestellt werden, inwieweit das geplante Vorgehen flexibel und responsiv genug ist, um Risiken in zunehmend software-definierten Netzwerken adäquat zu adressieren:

1. „Kritische Komponenten“ müssen zunächst durch den Katalog von Sicherheitsanforderungen nach § 109 Absatz 6 TKG näher bestimmt werden.
2. Kritische Komponenten „dürfen nur eingesetzt werden, wenn sie von einer anerkannten Prüfstelle überprüft und von einer anerkannten Zertifizierungsstelle zertifiziert wurden“ (§ 109 Absatz 2 TKG).
3. Betreiber müssen vor dem Einsatz einer kritischen Komponente zusätzlich eine Garantieerklärung des Herstellers beim Bundesministerium des Innern, für Bau und Heimat vorlegen.
4. Innerhalb eines Monats prüft das Bundesministerium des Innern, für Bau und Heimat die Garantieerklärung, u. a. basierend auf der Arbeit im interministeriellen Jour Fixe, und genehmigt oder untersagt den Einsatz.

5G-Netze sind zunehmend software-definiert, d. h. „kritische Komponenten“ sind meist Softwarekomponenten, deren Funktionalität zügig angepasst werden kann. Dieser zentrale Aspekt moderner Telekommunikationsnetze bleibt jedoch weitestgehend unberücksichtigt durch den engen Fokus auf Zertifizierung kritischer Komponenten. Bürokratische Kosten und Nutzen für die tatsächliche IT-Sicherheit unserer Telekommunikationsnetze stehen hier in einem schlechten Verhältnis.

Empfehlung: Die Norm § 9b BSIG-E sollte ersatzlos gestrichen und in ein separates Gesetzesvorhaben überführt werden.

9. Eingriff der Diensteanbieter in die Integrität von Kundensystemen

§ 7c BSIG-E Absatz 1 Satz 2 in Verbindung mit § 109a TKG Absätze 4,5 und 6

Es handelt sich hierbei um einen angeordneten Eingriff in das Computergrundrecht[28]. Es ist unklar, wie die operative Umsetzung aussähe und welche Schutzmechanismen ergriffen würden, um die Verfügbarkeit und Vertraulichkeit der betroffenen Datenverarbeitungssysteme durch die Veränderung der Integrität nicht zu beeinträchtigen. Darüber bietet diese Maßnahme im Sinne der IT- und Cybersicherheit keinen erkennbaren zusätzlichen Schutz zu den Maßnahmen gem. TKG § 109a Absätze 4, 5 und 6.

Empfehlung: § 7c BSIG-E Absatz 1 Satz 1 Nummer 2 sollte ersatzlos gestrichen werden.

10. Anordnungsbefugnis gegenüber Diensteanbietern

§ 7d BSIG-E

Es handelt sich hierbei um eine unpräzise gefasste Norm (Beispiel: „Vielzahl von Nutzern“). Dies ist vor dem Hintergrund eines möglicherweise hohen Erfüllungsaufwands problematisch.

Empfehlung: Diese Norm sollte weiter präzisiert werden.

11. Sonderrolle von Auswärtigem Amt und Bundeswehr und Mindeststandards nur im Einvernehmen

§ 4a BSIG-E Absätze 5 und 6 in Verbindung mit § 8 BSIG-E Absätze 1 und 1a und „Begründung“, „Besonderer Teil“

Mit § 4a BSIG-E werden zusätzliche Befugnisse geschaffen, damit das Bundesamt für Sicherheit in der Informationstechnik die IT-Sicherheit der Kommunikationstechnik des Bundes erhöhen kann. Die Begründung, warum gem. der Absätze 5 und 6 (Teile der) Informations- und Kommunikationsstruktur der Bundeswehr und das Auswärtige Amt hiervon ausgenommen werden sollen, ist aus IT-Sicherheitsperspektive schwer nachvollziehbar. Die Befugnisse des Bundesamtes für Sicherheit in der Informationstechnik sollen individuell über Verwaltungsvereinbarungen zwischen dem Bundesministerium der Verteidigung und dem Bundesministerium des Innern, für Bau und Heimat respektive dem Auswärtigen Amt und dem Bundesministerium des Innern, für Bau und Heimat geregelt werden, was die Transparenz einschränkt. Zusätzlich sollen Teile des Bundesministeriums der Verteidigung gem. §8 BSIG-E Absatz 1a von der Kontrolle und Überwachung des Mindeststandards für Sicherheit in der Informationstechnik des Bundes ausgenommen werden.

Während im Referentenentwurf vom 01.12.2020 das Bundesamt für Sicherheit in der Informationstechnik gem. § 8 BSIG-E Absatz 1 die Mindeststandards für die Sicherheit der Informationstechnik des Bundes im Benehmen mit den Ressorts festlegen konnte, soll das BSI das in der vorliegenden Version nur noch im Einvernehmen tun können. Die mögliche Schutzwirkung wird

[28] Bundesverfassungsgericht (2008): Leitsätze zum Urteil des Ersten Senats vom 27. Februar 2008- 1 BvR 370/07 -- 1 BvR 595/07 -

signifikant aufgeweicht, da Mindeststandards nicht mehr gegen den Willen der Ressorts erstellt werden können und die Ressorts sich stärker von anderen Interessen leiten lassen könnten.

Während die Ausnahmeregelung gem. § 4a BSIG-E Absatz 6 für die Bundeswehr – u. a. auf Basis der eigenen IT-Fähigkeiten im Organisationsbereich Cyber- und Informationsraum – nachvollziehbar erscheint, ist die Ausnahme des Auswärtigen Amts gem. § 4a Absatz 5 unverständlich und ggf. gefährlich. Das liegt sowohl an den, im Gegensatz zur Bundeswehr, begrenzteren eigenen IT-Fähigkeiten, sowie der Homogenität der IT-Systeme (z. B. keine Wehrtechnik), als auch – wie im Entwurf beschrieben – Cyberoperationen gegen das Ministerium. Gerade die Ausnahme des Auswärtigen Amtes wäre auf dieser Basis ein falsches Zeichen für die IT-Sicherheit in Deutschland.

Empfehlung: § 4a BSIG-E Absatz 5 sollte ersatzlos gestrichen werden, zumindest aber sollte die Verwaltungsvereinbarung öffentlich gemacht werden müssen. § 4a BSIG-E Absatz 6 müsste in der Begründung umfassender erklärt werden und die Verwaltungsvereinbarung sollte öffentlich gemacht werden müssen. Zu § 8 BSIG-E Absatz 1a letzter Satz sollte wie folgt abgeändert werden: „Im Geschäftsbereich des Bundesministeriums der Verteidigung sind die Mindeststandards für Informations- und Kommunikationstechnik im Sinne des § 4a Absatz 6 grundsätzlich umzusetzen. Nur begründet im Verteidigungsauftrag nach vorhergehender Risikoanalyse sind hier individuelle Ausnahmen möglich“.

Bereits im Rahmen des IT-Sicherheitsgesetzes hatte der Ausschuss für Inneres und Heimat 2015 in seinen Beschluss-Empfehlungen das Einvernehmen im damaligen § 8 BSIG durch das Benehmen ersetzt, da das Einvernehmenserfordernis die Schaffung eines einheitlichen Mindestsicherheitsniveaus faktisch verhindert.[29] Daher sollte § 8 BSIG-E Absatz 1 den Wortlaut des Referentenentwurfs in der Version vom 01.12.2020 enthalten, nämlich die Festlegung der Mindeststandards für die Sicherheit in der Informationstechnik des Bundes durch das Bundesamt für Sicherheit in der Informationstechnik mit den Ressorts im Benehmen.

12. Staatliche Cybersicherheitsarchitektur

„Begründung“, „Allgemeiner Teil“, „VI. Gesetzesfolgen“, „2. Nachhaltigkeitsaspekte“

Der Entwurf betrachtet weder die notwendigen Reformen der zentralen Akteure der deutschen Cybersicherheitsarchitektur – dem Nationalen Cyber-Abwehrzentrum und dem Cyber-Sicherheitsrat – noch die rechtliche Grundlage für die Zentrale Stelle für Informationstechnik im Sicherheitsbereich.

Empfehlung: Das IT-Sicherheitsgesetz 2.0 sollte genutzt werden, um die Strukturen des Nationalen Cyber-Abwehrzentrums und des Cyber-Sicherheitsrats zu klären und eine transparente rechtliche Grundlage für die Arbeit dieser Plattformen, und der Zentralen Stelle für Informationstechnik im Sicherheitsbereich, zu schaffen. Dies sollte unter anderem Kooperationsmöglichkeiten und -grenzen, Verantwortlichkeiten, Aufgaben und Verortung in der deutschen Cybersicherheitsarchitektur beinhalten. Hierzu gehört beispielsweise die Trennung zwischen operativen und nicht operativen Aufgaben im

[29] Deutscher Bundestag (2015): Beschlussempfehlung und Bericht des Innenausschusses (4. Ausschuss) zu dem Gesetzentwurf der Bundesregierung – Drucksache 18/4096 – Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz)

Bereich der Cybersicherheit (vgl. u. a. BVerfG Leitsätze zum Urteil des Ersten Senats vom 19. Mai 2020)[30]. Weiterhin sollte die Bundesregierung einen Plan zur Weiterentwicklung der deutschen Cybersicherheitsarchitektur vorlegen, insbesondere vor dem Hintergrund der Gründung immer neuer Institutionen wie der Zentralen Stelle für Informationstechnik im Sicherheitsbereich, der Agentur für Sprunginnovationen, der Cyberagentur, dem Zentrum für Digitalisierungs- und Technologieforschung der Bundeswehr und vielen mehr, und damit möglicherweise entstehender unklarer Verantwortlichkeiten und Parallelstrukturen entgegenwirken.

C. Empfehlung

Durch die Weiterentwicklung der Gefährdungslage seit dem letzten IT-Sicherheitsgesetz ist es dringend geboten die IT-Sicherheitsgesetzgebung weiter zu verbessern. Aufgrund der bevorstehenden Bundestagswahlen 2021 – und dem selbstverschuldeten Zeitdruck der Bundesregierung – wäre es für die IT-/Cybersicherheit in Deutschland wichtig eine entsprechende Gesetzgebung noch im ersten Halbjahr 2021 zu verabschieden. Wie dargestellt beinhaltet der vorliegende Entwurf jedoch noch elementare Schwächen und bedarf weiterer Überarbeitung.

Folgendes Vorgehen würde aus hiesiger Sicht daher den kleinsten gemeinsamen Nenner darstellen:

1. Die Übernahme folgender Empfehlungen in den Gesetzestext ist dringend geboten:

„8. Kritische Komponenten und vertrauenswürdige Hersteller“

„9. Eingriff der Diensteanbieter in die Integrität von Kundensystemen“

„11. Sonderrolle von Auswärtigem Amt und Bundeswehr und Mindeststandards nur im Einvernehmen“

2. Die Übernahme folgender Empfehlungen kann in der Cybersicherheitsstrategie 2021 erfolgen:

„2. Evaluierung der bisherigen IT- und Cybersicherheitsmaßnahmen“

„12. Staatliche Cybersicherheitsarchitektur“

3. Die Übernahme folgender Empfehlung kann durch Einführung eines staatlichen Schwachstellenmanagements im Jahr 2021 erfolgen:

„5. Schwachstellenmanagement und -meldewesen“

4. Die Übernahme folgender Empfehlungen sollte im Rahmen der NIS-Richtlinie II erfolgen:

„1. IT-Sicherheit für die Gesellschaft durch Verbraucherschutz“

„4. Unternehmen im besonderen öffentlichen Interesse und Parteien“

Weiterhin sollte die Bundesregierung Schritte ergreifen, damit Gesetzgebung in diesem Bereich zukünftig strategischer, empirisch-fundierter, partizipativer und inklusiver ist. Das beinhaltet angemessene Kommentierungsfristen, ebenso wie die Bereitstellung von Synopsen und eine angemessene Zeitplanung (u. a. nicht parallele Notifizierung der EU und Parlamentsbefassung kurz vor einer Bundestagswahl).

[30] Bundesverfassungsgericht (2020): Leitsätze zum Urteil des Ersten Senats vom 19. Mai 2020 - 1 BvR 2835/17 – [5. Leitsatz]

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
19(4)741 C

AG KRITIS

Stellungnahme für die Anhörung des Bundestagsausschusses für Inneres und Heimat

Entwurf eines Zweiten Gesetzes zur Erhöhung der Sicherheit Informationstechnischer Systeme 2.0 (IT-Sicherheitsgesetz 2.0)

am 01.03.2021

Manuel Atug

Gründer und Sprecher der unabhängigen AG KRITIS

Der Sachverständige dankt allen ehrenamtlich tätigen Expert:innen der AG KRITIS und den vielen Sicherheitsforscher:innen aus der Community für ihre Unterstützung.

Kontakt

Manuel Atug

E-Mail: HonkHase@ag.kritis.info

Twitter: @HonkHase

Webseite: https://ag.kritis.info

Inhalt

Vorbemerkungen zum bisherigen Verfahrensablauf....3
Qualität der Strategie und der Ziele im IT-SiG 2.0....4
Harmonisierung mit der EU....5
Dreigespann an Kritikalität....5
UNBÖFI einschließlich Rüstungsindustrie....6
Zurückhalten von Schwachstellen....7
Hackerparagraphen und die Frage der Haftung bei offensiven und invasiven BSI Handlungen....9
Neutralitätsdefizit des BSI....10
Digitale Souveränität & Kritische Komponenten....11
Digitale Souveränität & der Detailgrad....13
Digitale Souveränität & Open Source Untersagung....14
EU Cyber Security Act (CSA) und freiwilliges IT-Sicherheitskennzeichen....14
Sanktionen & (nicht vorhandene) Incentivierungen....15
Ausstehende Evaluierung des IT-SiG 1.0....15
Gestrichene Themen und Optimierungspotential....18
Symptomatisch handlungsunfähig im Cyberraum....19
Fazit....22

Vorbemerkungen zum bisherigen Verfahrensablauf

Über zwei Jahre hat das BMI hinter verschlossenen Türen vor sich hin gewerkelt und mit Referaten anderer Ministerien zu überaus umfangreichen Befugniserweiterungen verhandelt, so dass die Verhandlungsbasis eine überdimensioniert schwierige Ausgangsbasis dargestellt hat. Im ersten Quartal 2019[1] und im zweiten Quartal 2020[2] ist jeweils ein Referentenentwurf vorab geleaked worden, da eine Beteiligung der Wissenschaft, Wirtschaft, Zivilgesellschaft und Sicherheitsforscher:innen in diesem Zeitraum trotz derer wiederholten Bitten weder vorgesehen noch berücksichtigt wurde.

Diese Leaks war in den zwei Jahren somit leider der einzige Weg, dass auch Wissenschaft, Wirtschaft, Zivilgesellschaft und Sicherheitsforscher:innen sich frühzeitig einlesen und eigene Gedanken zum kommenden IT-SiG 2.0 machen können. Ein aktives einbringen war dabei zu den Zeitpunkten ebenfalls weder möglich noch vorgesehen.

Das BMI hat erst am 9.12.2020[3] erstmalig eine öffentlich verfügbare Verbändefassung auf ihrer Webseite bereitgestellt, um Betroffenen, Interessierten und fachkundigen Dritten die Beteiligung durch initiale Einsichtnahme zu ermöglichen.

Als das Verfahren diesen offiziellen Charakter angenommen hatte, ging es dann plötzlich Schlag auf Schlag. Von 19.11.2020 bis 16.12.2020 alleine gab es fünf veröffentlichte Versionen mit teils umfangreicheren Anpassungen[4], die aber in Teilen wiederum nur einigen beteiligten Wirtschaftsverbänden bereitgestellt wurden. Hierbei wurden an einigen Stellen betroffene Verbände nicht berücksichtigt, so dass diese in ihrer Stellungnahme darauf verwiesen hatten, dass sie eigeninitiativ reagieren mussten und daher nicht die angemessene Zeit erhalten hatten, um eine vollständige Analyse und Kommentierung vorzunehmen.

Dabei wurden grundsätzlich alle neuen Versionen des Gesetzesentwurfs lediglich als nicht editierbares PDF-Dokument ohne Hervorhebung von Änderungen bereitgestellt. Eine Synopse mit einfachem aufzeigen oder transparent erfolgtem Abgleich der Veränderungen wurde zu keinem Zeitpunkt ermöglicht.

Dies kam insbesondere bei der letzten Änderung zur Wirkung[5], so dass Stellungnahmen nicht mehr angepasst werden konnten, denn der Zeitraum zwischen Bereitstellung der überarbeiteten Version mit über 100 Seiten Text an Gesetzesentwurf und Fristablauf zur Einreichung der Stellungnahme hatte zuletzt dann auch nur noch unverschämte 26 Stunden Reaktionszeit beinhaltet.

Die AG KRITIS stellte hierzu bereits berechtigt fest: ***Eine so kurze Frist ist der ministerielle Mittelfinger ins Gesicht der Zivilgesellschaft!***[6]

Trotz dieser umfangreichen Widrigkeiten zur aktiven Verhinderung einer Beteiligung an diesem zukunftsweisenden Gesetz im Kontext der Cybersicherheit und digitalen Souveränität Deutschlands haben insgesamt 24 Stellungnahmen aus der privaten Wirtschaft sowie aus den

[1] https://ag.kritis.info/wp-content/uploads/2020/12/20190327-IT-Sicherheitsgesetz-2.0.pdf
[2] https://ag.kritis.info/wp-content/uploads/2020/12/20200507-IT-Sicherheitsgesetz-2.0.pdf
[3] https://ag.kritis.info/wp-content/uploads/2020/12/20201209-IT-Sicherheitsgesetz-2.0.pdf
[4] https://ag.kritis.info/2021/02/22/it-sicherheitsgesetz-2-0-alle-verfuegbaren-versionen/
[5] https://ag.kritis.info/wp-content/uploads/2020/12/20201211-IT-Sicherheitsgesetz-2.0.pdf
[6] https://ag.kritis.info/2020/12/09/it-sicherheitsgesetz-2-0-vierter-entwurf-jetzt-vom-bmi-nur-noch-24h-zeit-zur-kommentierung/

zivilgesellschaftlichen und sonstigen Organisationen das BMI erreicht.[7] Bedarf zur Beteiligung ist also offensichtlich umfassend vorhanden, nur hebt das BMI dieses Potenzial nicht, sondern lässt es brach liegen.

Diese umfassende Beteiligung macht aber die Bedeutung und Kritikalität des Gesetzes mehr als deutlich und das Versagen bei der effektiven Ermöglichung einer Beteiligung umso schwerwiegender. Ganz abgesehen davon, dass das BMI hier noch viel umfassendere Fachexpertise aus verschiedenen Blickwinkeln hätte frei Haus erhalten können.

So - und nur so - kann im Übrigen ein Stand der Technik[8], welcher schon im IT-SiG 1.0 verankert ist, erreicht werden.

Qualität der Strategie und der Ziele im IT-SiG 2.0

Das IT-SiG 2.0 zeigt unter anderem auch und insbesondere aufgrund dieser Vorgehensweise eine **eklatante Strategie- und Ziellosigkeit** des Gesetzgebers im Cyberraum auf.

Deutlich wird dabei auch an vielen Stellen der Konflikt der „Sicherheit“ aus Sicht der Sicherheitsbehörden und Nachrichtendienste im Kontext der Befugniserweiterungen und der Gefahrenabwehr auf der einen Seite. Und auf der anderen Seite „Sicherheit“ im Kontext der Erhöhung der Cyberresilienz aus KRITIS-Sicht, also der Sicht der robusten und widerstandsfähigen Versorgung der Zivilbevölkerung. Die im Übrigen auch genau deswegen in dieser Form im IT-SiG 1.0 in § 2 Abs. 10 BSIG[9] eingebracht wurde:

„Kritische Infrastrukturen im Sinne dieses Gesetzes sind […] von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden.“

Untermauert wird diese beschriebene eklatante Strategie- und Ziellosigkeit darüber hinaus auch noch durch die immer noch ausstehende - gesetzlich vorgeschriebene[10] - Evaluierung der Wirksamkeit des IT-SiG 1.0. Ein IT-SiG 2.0 einzuführen, ohne das IT-SiG 1.0 analysiert zu haben und den daraus resultierenden Erkenntnisgewinn als Feedback einzubringen, zeugt von einer grundsätzlichen und prozessbedingten verminderten Qualität durch Kardinalsfehler im Prozessablauf.

Der vorgelegte Gesetzesentwurf lässt daher keine klare Linie zur konsequenten Erhöhung des Sicherheitsniveaus der IT-Systeme und Kritischen Infrastrukturen erkennen. Im gesamten Gesetzestext ist keine Strategie erkennbar, grundlegende Sicherheitsanforderungen zu stärken.

Vielmehr scheint es sich um eine bunte Mischung - teilweise sachfremder - Wünsche seitens einzelner Behörden zu handeln. Grundlegende Maßnahmen, die sinnvoll wären, wie die eindeutige

---

[7] https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/entwurf-zweites-it-sicherheitsgesetz.html

[8] https://www.bmjv.de/SharedDocs/Downloads/DE/Themen/RechtsdurchsetzungUndBuerokratieabbau/HandbuchDerRechtsfoermlichkeit_deu.pdf?__blob=publicationFile&v=2

[9] https://www.gesetze-im-internet.de/bsig_2009/BJNR282110009.html

[10] https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&start=//*%255B@attr_id=%27bgbl115s1324.pdf%27%255D#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl115s1324.pdf%27%5D__1614244823027

und klarstellende verpflichtende Einführung eines Informationssicherheitsmanagementsystems (ISMS) mit Business Continuity Management (BCM) sind weiterhin nicht explizit erwähnt. Gute Ideen aus vorherigen Referentenentwürfen fehlen ganz, dafür wurden mehrere verfassungsrechtlich höchst fragliche Passagen hinzugefügt.

Das IT-SiG 2.0 droht insofern eine Sammlung von unabgestimmten und insbesondere ineffektiven Maßnahmen mit zahlreichen Redundanzen und Mehrfachregulierungen zu werden, die in Teilen keinen Sinn ergeben und keine klare Zielrichtung vorgeben. Es ist daher zu erwarten, dass dies darüber hinaus sogar Verwirrung stiften und Unklarheit fördern wird. So wird die geplante mehrspurige Autobahn zu einer Motocross Strecke wo jeder querfeldein agiert.

Aus Sicht der AG KRITIS kommt darüber hinaus die Kernidee des Schutzes kritischer Infrastrukturen (KRITIS) angesichts der Tatsache, dass KRITIS im IT-SiG 1.0 im Vordergrund standen, viel zu kurz. Was bedenklich stimmt ob der vermeintlichen und tatsächlichen Ziele des IT-SiG 2.0.

In Teilen wird dadurch sogar die Sicherheit gemindert, statt sie zu erhöhen. Das kann und darf kein Ergebnis dieses Prozesses und des daraus resultierenden Gesetzes sein!

Harmonisierung mit der EU

Im Übrigen ist im Entwurf eine EU Sicht und Angleichung oder Harmonisierung ebenfalls nicht als Strategie erkennbar.

Beispielsweise gibt es den deutschen Alleingang in § 9c BSIG „Freiwilliges IT-Sicherheitskennzeichen“ zusätzlich zur EU CSA Umsetzung in § 9a BSIG „Nationale Behörde für die Cybersicherheits-zertifizierung“.

Auch „Unternehmen im besonderen öffentlichen Interesse“ (UNBÖFI) stellen eine neue Kategorie parallel zu KRITIS dar, welche die EU ebenfalls weder in der EU NiS-Richtlinie[11] vorsieht noch auf sonstige Weise kennt oder vorsieht.

Dreigespann an Kritikalität

Offenbar sieht das IT-SiG 2.0 eine nicht sehr sinnvolle aber dafür verdeckte Dreiteilung von Schutzkategorien im Cyberraum Deutschlands vor:

1. **Besonders Kritisch**
   Hierbei handelt es sich um KRITIS Betreiber mit kritischen Komponenten gemäß § 9b BSIG
2. **Kritisch**
   Hierbei handelt es sich um KRITIS Betreiber nach § 2 Abs. 10 BSIG
3. **Leicht kritisch**
   Dies sind UNBÖFI nach § 2 Abs. 14, im umgänglichen Sprachgebrauch auch oft als „KRITIS light“ bezeichnet

[11] https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32016L1148

Die Sinnhaftigkeit hieraus erschließt sich nicht, denn der Schutzbedarf und ein daraus abgeleiteter Umfang von Maßnahmen ergibt sich aus der in § 8a BSIG vorgesehenen Methodik zur Umsetzung: *„angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen“*, sprich der eigentlich klassischen Umsetzung eines ISMS mit BCM nach Stand der Technik, die aber so explizit nicht in den Gesetzestext hineinformuliert wurde.

UNBÖFI einschließlich Rüstungsindustrie

Das IT-SiG 2.0 soll in § 2 Abs. 14 BSIG um drei verschiedenen Arten von Unternehmen erweitert werden, die nicht KRITIS Betreiber sind:

> *„1. die Güter nach § 60 Absatz 1 Nummer 1 und 3 der Außenwirtschaftsverordnung in der jeweils geltenden Fassung herstellen oder entwickeln,*
>
> *2. die nach ihrer inländischen Wertschöpfung zu den größten Unternehmen in Deutschland gehören und daher von erheblicher volkswirtschaftlicher Bedeutung für die Bundesrepublik Deutschland sind oder*
>
> *3. die Betreiber eines Betriebsbereichs der oberen Klasse im Sinne der Störfall-Verordnung in der jeweils geltenden Fassung sind oder nach § 1 Absatz 2 der Störfall-Verordnung diesen gleichgestellt sind.“*

Unter die Definition *„die Güter nach § 60 Absatz 1 Nummer 1 und 3 der Außenwirtschaftsverordnung“* fällt unter anderem auch die deutsche Rüstungsindustrie.

Die deutsche Rüstungsindustrie wird hier allerdings politisch strategisch mit dem Schutz der Zivilbevölkerung in Deutschland vermengt. Sie ist daher in anderen Gesetzen zu berücksichtigen und sollte aus der Sicht der nationalen Sicherheit adressiert werden und unter dem Kontext angemessene Berücksichtigung finden. Aber keinesfalls im Kontext des Zivilschutzes und der zivilen Fragestellungen und nur nach UNBÖFI-Vorgaben, die für diese Kritikalität viel zu unzureichend ausgestaltet sind.

UNBÖFI ist allerdings auch insgesamt als nichts Ganzes und nichts Halbes zu betrachten. Abgesehen davon, dass die militärnahe Rüstungsindustrie in Zivilgesetzen Einzug erhält und in unangemessener Weise Berücksichtigung finden soll, wird durch die Hintertür eine Art „KRITIS light“ eingeführt.

Was dieses „KRITIS light“ dabei genau sein soll und nach welchen genauen Kriterien ein Unternehmen UNBÖFI wird, ist nicht im Gesetz abgedeckt, sondern soll durch eine noch unbekannte Rechtsverordnung festgelegt werden. Diese ist allerdings nicht einmal im Entwurf öffentlich verfügbar. So wird es auch hier wieder ein intransparentes Verfahren. Und dann eben hoffentlich auch eine Verordnung, die auch ohne den Einbezug von Fachexpertise der Wissenschaft, Wirtschaft, Zivilgesellschaft und Sicherheitsforscher:innen in der ersten gültigen Fassung gut wird.

Unter die Definition *„Betreiber eines Betriebsbereichs der oberen Klasse im Sinne der Störfall-Verordnung“* fallen unter anderem auch deutsche Unternehmen nach Störfall-Verordnung wie z. B. Chemieunternehmen. Aber auch Heizöl-Tanklager oder Raffinieren - die zwar als KRITIS erfasst sind, wenn sie über dem aktuellen Schwellenwert der BSI-Kritisverordnung[12] liegen, aber nicht, wenn sie darunter liegen.

Diese müssen dann allerdings - entgegen der KRITIS Betreiber - nur Teile der Maßnahmen und Vorgaben abdecken, da sie nicht als KRITIS sondern lediglich als UNBÖFI eingestuft werden.

Folgende Frage drängt sich daher naturgemäß auf: Wieso können Störfall-Verordnung relevante Unternehmen eigentlich UNBÖFI statt KRITIS sein?

Aus dem Schutz vor Gefahren einer Anlage ausgehend sollte auch Gefahr als KRITIS relevant angesehen werden. Verpflichtungen für Unternehmen nach Störfall-Verordnung müssten daher gleichwertig sein wie bei KRITIS Betreibern und diese dann damit eben nicht nur als UNBÖFI sondern immer als KRITIS eingestuft werden.

Dies bedeutet, dass diese Unternehmen daher nicht als KRITIS Betreiber berücksichtigt oder die Anforderungen gleichgesetzt wie bei KRITIS werden, da dann die gleichen angemessenen Anforderungen an deren IT-Sicherheit fällig werden.

Wenn diese Unternehmen aus dem Schutzbedarf so relevant sind, dass es eine Störfall-Verordnung gibt, wieso findet dann die IT Sicherheit nicht angemessene Berücksichtigung?

Die Berücksichtigung von unter die Störfall-Verordnung fallenden Unternehmen als UNBÖFI greift daher viel zu kurz. Denn diese Unternehmen stellen durch die Verarbeitung eine große Gefahr für die Zivilbevölkerung dar, daher sind für unter die Störfall-Verordnung fallenden Unternehmen nach § 8f BSIG auch die Anforderungen von § 8a BSIG vorzugeben.

Zurückhalten von Schwachstellen

Nach § 7b Abs. 3 BSIG sind die für den Betrieb eines IT-Systems verantwortlichen über die bei einem Scan des BSI gefundenen Sicherheitslücken bzw. Sicherheitsrisiken nur dann zu informieren, wenn „überwiegende Sicherheitsinteressen“ dem nicht entgegenstehen. Dies legt erneut den Verdacht nahe, dass es für das BSI als eine dem BMI unterstellte Behörde, Interessenkonflikte gibt. Diese Regelung schafft keinen rechtlichen Rahmen für den verantwortungsvollen Umgang mit Sicherheitslücken.

Als IT-Sicherheitsbehörde sollte das BSI sowohl Betreiber unsicherer Systeme als auch Hersteller von IT-Produkten immer über alle gefundenen Schwachstellen und Sicherheitslücken gemäß Responsible Disclosure Verfahren informieren. So sind diese in der Lage, mitigierende Maßnahmen einzuleiten und den Schutz der IT-Systeme aufrecht halten. Dies stellt eine konkrete Erhöhung der IT-Sicherheit dar.

Es ist aus dem Gesetzentwurf auch nicht ersichtlich, welche „überwiegenden Sicherheitsinteressen“ dem entgegenstehen sollten.

Da unsichere IT-Systeme nicht nur für Betreiber und Kunden - also die Zivilgesellschaft und die Wirtschaft - eine Gefahr darstellen, sondern auch von Angreifern für Attacken auf weitere Dritte

[12] https://www.gesetze-im-internet.de/bsi-kritisv/BJNR095800016.html

dienen können, müssen diese Unsicherheiten bedingungslos und konsequent abgestellt werden. Auch darum sind Betreiber der Systeme immer und über jeden möglichen Kanal gemäß Responsible Disclosure Verfahren zu informieren.

Der Gesetzentwurf legt nahe, dass dies das alleinige Ziel von § 7b BSIG ist.

Das BSI soll allerdings darüber hinaus durch Art. 10 GG geschützte Informationen ausschließlich zum Zwecke der Übermittlung nach § 5 Abs. 5 und 6 BSIG - also zur Weitergabe an die Polizeien und Nachrichtendienste - verwenden dürfen. Im Vordergrund darf aber nicht die Anreicherung von sensitiven Datenbergen (Stichwort Vorratsdatenspeicherung) bei Polizeien und Nachrichtendiensten stehen.

Hier ist selbstverständlich die Beseitigung von Sicherheitslücken vorrangig. Der entsprechende Satz ist daher ersatzlos zu streichen. Im darauffolgenden Satz ist weiterhin klarzustellen, dass die Art. 10 GG-Informationen (wie z.B. IP-Adressen) ausschließlich zur Warnung der Betroffenen verwendet werden dürfen und anschließend sofort vom BSI unwiederbringlich zu löschen sind.

Generell wird festgestellt, dass der Gesetzentwurf erstaunlich oft auf die Regelungen zur Weitergabe von Informationen über Schwachstellen und Sicherheitsprobleme an Polizeien und Nachrichtendiensten nach § 5 Abs. 5 und 6 BSIG verweist. So sollen an diese nach § 4b Abs. 2 BSIG auch Informationen über die Identität von Meldenden weitergegeben werden. Das dient nicht dem Zweck der IT-Sicherheit und hat in einem IT-Sicherheitsgesetz daher auch nichts zu suchen. Die digitale Souveränität in Deutschland lässt auch hier wieder deutlich Federn.

Das legt wiederum deutlich nahe, dass das BSI als Handlanger der Sicherheitsbehörden bzw. konkret der Polizeien und Nachrichtendienste instrumentalisiert werden soll. Dies wird nicht dadurch besser, dass Verfassungsschutz und Polizeibehörden Staatstrojaner einsetzen dürfen und dafür Schwachstellen benötigen, sowie dass die ZITiS ebenfalls Schwachstellen benötigt, um Sicherheitsbehörden und Nachrichtendienste zu unterstützen.

Das Gesetz sollte daher klarstellen, dass dem BSI gemeldete Informationen ausschließlich für den Schutz der IT-Sicherheit verwendet werden dürfen und der Einsatz oder die Verwendung für offensive oder invasive Zwecke nicht zulässig ist.

Um ein hohes Maß an IT-Sicherheit erreichen zu können, sind alle Sicherheitsbehörden wie z. B. BND, BKA, Bundespolizei, Verfassungsschutz, ZITiS und die Bundeswehr zu verpflichten, von ihnen gefundene oder erworbene Schwachstellen ausnahmslos an das BSI zu melden.

Es braucht diese ausnahmslose Meldepflicht entdeckter Sicherheitslücken, die für alle staatlichen Stellen gelten muss. Ohne ein solch klares Bekenntnis des Gesetzgebers - auch zur Rolle des BSI hin - droht ansonsten ein schwerwiegender Vertrauensverlust bei den relevanten Akteuren aus der Wissenschaft, Wirtschaft, Zivilgesellschaft und den Sicherheitsforscher:innen.

Der regelmäßige Austausch mit Sicherheitsforscher:innen zeigt bereits, dass viele aufgrund herrschender Vorbehalte nicht (mehr) gewillt sind, entdeckte Schwachstellen und Sicherheitslücken an das BSI zu melden, weil das BSI eben nicht gesetzlich unabhängig nur für Sicherheit im Sinne der Defensive und der Cyberresilienz steht, sondern klar davon auszugehen ist, dass es für das BMI und die nachgelagerten Sicherheitsbehörden auch zur Unterstützung der Offensive und den invasiven Tätigkeiten beiträgt - Beispielsweise durch das hier geforderte Zurückhalten von Schwachstellen.

Auch die private Wirtschaft und insbesondere KRITIS Betreiber trauen dem BSI nicht mehr vollständig, was sehr gefährliche Züge für die Gesamtsicherheit in Deutschland annimmt, da IT-Sicherheit vom vertrauensvollen Austausch aller Akteure lebt. Vertrauen wird nun mal mühselig

und langwierig aufgebaut, kann aber durch solche Handlungen oder Gesetzesinhalte schnell zerstört werden...

Das Zurückhalten von Sicherheitslücken ist darüber hinaus gar nicht erforderlich, denn bekannt gewordene Sicherheitslücken werden ohnehin nicht umgehend flächendeckend geschlossen. Sicherheitsbehörden und Geheimdienste könnten daher alle bekannten offenen und ungepatchten Lücken nutzen, bis deren Ziele diese gepatcht haben.

Wird dies nicht vollständig berücksichtigt, wird der Staat seiner Verantwortung in der Digitalisierung und in eine digitale Souveränität Deutschlands nicht gerecht!

Eine einfache aber relevante Regel lautet: Die Zurückhaltung von Schwachstellen betrifft immer(!) auch die Zivilgesellschaft weltweit(!) sowie auch die private Wirtschaft und KRITIS Betreiber weltweit(!).

Im Hinblick auf die möglichen Folgen von Ausfällen kann das Offenhalten oder Verzögern der Behebung von Sicherheitslücken in einer Gesamtabwägung daher niemals angemessen sein. Wichtig ist in diesem Zusammenhang insbesondere, dass Betroffene wie die KRITIS-Betreiber vom BSI schnellstmöglich über sie betreffende IT-Sicherheitslücken informiert werden.

Wie stark soll denn sonst der Vertrauensverlust in den demokratischen Rechtsstaat werden?

Wie auch von anderen Stellen bereits gefordert, sollten die zusätzlichen Kompetenzen des BSI einer umfassenden Transparenz und Kontrolle unterliegen. Eine Trennung der Aufsicht über defensive durch das BSI und Offensive bzw. invasive durch die Sicherheitsbehörden und Nachrichtendienste würde das Vertrauen in das BSI deutlich erhöhen.

Dass Menschen mehr Hilfestellung im Bereich IT-Sicherheit wünschen, wundert ja grundsätzlich nicht. Selbst Informatiker:innen und Sicherheitsforscher:innen scheitern an den maroden Benutzerinterfaces von angeflanschter Security. Integrierte Sicherheit nach dem Modell „Security by Design“ ist eben Mangelware, da der Motivator für Unternehmen fehlt. Unsichere Software („Insecure by lack of Design“) ist dafür wiederum überall verfügbar, aber eher getreu dem Designprinzip „Fail by Design“.

Der Staat fördert das nicht, wenn er Backdoors, Frontdoors und Staatstrojaner - z. B. via ZITiS - für Polizeibehörden, Nachrichtendienste und Militär gesetzlich legitimiert und auf dem 0day Trading Graumarkt einkaufen oder selbst erforschen und entwickeln lässt.

Denn wenn IT-Systeme und Software aufgrund von Lawful Interception Maßnahmen und Staatstrojanern „defekt by Design“ sind, was bringt dann ein vermeintlich sicher entwickeltes System? Es müsste ja doch wieder für die Vorgaben vom deutschen Staat zur Fütterung seiner Sicherheitsbehörden und Nachrichtendienste aufgebrochen werden...

Hackerparagraphen und die Frage der Haftung bei offensiven und invasiven BSI Handlungen

§ 7c Abs. 1 Nr. 2 BSIG sieht vor, dass technische Befehle zum Zwecke einer Fehlerbereinigung an betroffene IT-Systeme von Betreibern verteilt werden können, welche das BSI allerdings nicht im genauen Betriebs- und Konfigurationszustand kennt. Dies birgt Risiken bei der Veränderung der IT-Systeme mittels der hierbei vorgesehenen invasiven Eingriffsmöglichkeiten.

Führt das BSI gemäß § 7b BSIG z. B. Scans durch, haftet der Staat für ggf. eintretende Fehlerzustände der IT-Systeme. Aber wer trägt aufkommende Kosten für das Auslösen einer Notfallprozedur? Beispielsweise bei einem KRITIS Betreiber?

Und wie erfährt z. B. solch ein KRITIS Betreiber davon, dass das BSI gescannt hatte und die Ursache für den Ausfall war? Wie kann er also die Ansprüche dafür geltend machen?

Und was ist mit dem daraus resultierenden Risiko von drohendem Versorgungsengpass oder gar Versorgungsausfall der kritischen Dienstleistung wie z. B. Strom und Wasser bei KRITS Betreibern? Was sieht der Gesetzgeber dann für den betroffenen Teil der Bevölkerung vor? Stellt er Notstrom und Wasserrationen deutschlandweit in die Bevorratung und hält diese für solche Szenarien vor?

Es gibt immer wieder bestätige und validierte Vorfälle, wo IT-Systeme und Netzwerkkomponenten nach einem Scan in einen Fehlerzustand fallen, rebooten oder sogar komplett einfrieren. Ja, solche Systeme sind auch direkt und ungefiltert an das Internet angebunden. Wurde die dafür erforderliche Ethik in Netzwerk Systemen daher hinreichend berücksichtigt und vorgegeben, z. B. „Philosophy meets Internet Engineering: Ethics in Networked Systems Research“[13] oder „Network Systems Ethics Guidelines“[14]?

Das BSI sollte daher mindestens solche Konzepte entwickeln, die diese Risiken adressieren. Diese sind als Vorgabe im Gesetzesentwurf mit aufzunehmen.

Grundsätzlich gilt aber: Invasiv auf IT-Systemen agieren ist gefährliches und nicht hervorsagbares rumpfuschen und stellt eine OP am offenen Herzen dar. Dies ist daher die schlechteste Variante einer Umsetzungsmöglichkeit zur Zielerreichung und darüber hinaus auch nicht notwendig!

Die relevanten Gefahren können mittels angemessener Gefahrenabwehr nach § 7c Abs. 1 Nr. 1 BSIG dargestellt und adressiert werden. Sogar ein MIRAI Botnetz[15] kann damit abgedeckt werden.

Neutralitätsdefizit des BSI

Der Schutz Kritischer Infrastrukturen als auch die Erhöhung von IT-Sicherheit sind auf die Zusammenarbeit von Wissenschaft, Wirtschaft, Zivilgesellschaft und Sicherheitsforscher:innen im Allgemeinen angewiesen.

Eine fehlende Neutralität der staatlichen und für KRITIS zuständigen Aufsichtsbehörde mindert das essentiell notwendige Vertrauen unnötig und behindert so diesen essentiellen Austausch durch die Zusammenarbeit für das gemeinsame Ziel.

Das BSI stellt sich oftmals als neutral und unabhängig in der Außendarstellung dar. Diese Unabhängigkeit ist aber faktisch nicht gegeben, solange es gemäß § 1 Satz 2 BSIG dem BMI unterstellt ist: *„Es untersteht dem Bundesministerium des Innern, für Bau und Heimat.“*

Das BSI ist innerhalb des BMI der Abteilung CI, Cyber- und Informationssicherheit zugeordnet. Diese Abteilung adressiert des Weiteren sowohl „Wirtschaft und Gesellschaft“ als auch die Sicherheitsbehörden, das BfV und das BKA.

[13] https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/41/2015/09/ENSR-Oxford-Workshop-report.pdf
[14] http://networkedsystemsethics.net/index.php?title=Networked_Systems_Ethics_-_Guidelines
[15] https://de.wikipedia.org/wiki/Mirai_(Computerwurm)

Diese beiden Gruppen von Behörden haben oftmals diametrale Ziele, so dass zwei konträre Herzen in einer Brust an einer zentralen Stelle im BMI schlagen und Zielkonflikte dadurch vorprogrammiert sind. Bei der oben aufgezeigten Gewichtung wird deutlich, wie ein Pendel „Sicherheit im defensiven Sinne eines BSI“ vs „Sicherheit im Sinne von Ermittlungs- und Sicherheitsbehörden als auch nachrichtendienstlicher Behörden“ innerbehördlich ausschlagen wird, so dass berechtigt von einem systemimmanenten Neutralitätsdefizit gesprochen werden muss.

Das BSI hat daher Ultima Ratio die Vorgaben des BMI einzuhalten und auszuführen und agiert somit weder neutral noch unabhängig. Die Option des Einwirkens wird durchaus auch seitens BMI bei Bedarf gezogen, wie z. B. bei der angeordneten Unterstützung für den Staatstrojaner vor einigen Jahren oder auch durch aktives Zurückhalten von Schwachstellen.

Der Koalitionsvertrag aus der 19. Legislaturperiode besagt interessanter Weise im Widerspruch hierzu auf Seite 44 ab Zeile 1970:

„Wir wollen das BSI als nationale Cybersicherheitsbehörde ausbauen und in seiner Rolle als unabhängige und neutrale Beratungsstelle für Fragen der IT-Sicherheit stärken“

Um das Ziel der Unabhängigkeit und Steigerung des Vertrauens zu erreichen ist zwingend erforderlich, dass das BSI mindestens(!) eine fachliche Unabhängigkeit vom BMI erhält, wie sie zum Beispiel das statistische Bundesamt erhalten hat. Konkret ist daher § 1 Satz 2 BSIG zur Grundlage technisch-wissenschaftlicher Erkenntnisse unter Einbezug von fachlich verantwortlichen Ministerien wir folgt anzupassen:

"Das BSI führt seine Aufgaben auf der Grundlage wissenschaftlich-technischer Erkenntnisse nach den Anforderungen der jeweils fachlich zuständigen Ministerien durch."

Diese Maßnahme stärkt das notwenige Vertrauen, welches für die Zusammenarbeit von Wissenschaft, Wirtschaft, Zivilgesellschaft und Sicherheitsforscher:innen im Allgemeinen notwendig ist.

Digitale Souveränität & Kritische Komponenten

§ 9b BSIG führt kritische Komponenten ein und fordert zünftig eine Vertrauenswürdigkeitserklärung von Herstellern kritischer Komponenten.

Dabei ist schon der Begriff und das Verständnis, was genau eine kritische Komponente ist und was sie wiederum nicht ist, nicht ausreichend rechtlich begriffsbestimmt. Wie wird also diese ominöse Vertrauenswürdigkeit rechtssicher definiert und wie kann diese überhaupt in einer Form überprüft werden, die dem Anspruch und der Intention dahinter genügen kann?

Es drängt sich daher die Frage auf, was das Ziel der Zertifizierung von kritischen Komponenten ist, wie dies funktionieren soll und ob dies generell Sinn macht. Mit einer Zertifizierung kann das Einschmuggeln einer Sicherheitslücke durch fremde Nachrichtendienste nicht vermieden werden. Welche Hoffnung soll also damit verbunden und was genau verhindern werden?

Darüber hinaus stellt sich die Frage, warum sich diese Regelung im Gegensatz zu den anderen IT-SIG Regelungen nicht auf alle KRITIS Betreiber sondern auf ausgewählte Komponenten von einigen KRITIS Sektoren beziehen soll.

Dasselbe Unternehmen könnte im Übrigen auch als nicht vertrauenswürdiger Hersteller kritischer Komponenten eingestuft und trotzdem KRITIS Betreiber sein, wenn es z. B. Software defined Radio oder Software defined Networking selber entwickelt.

Müsste ein solches Unternehmen diese kritischen Komponenten dann aber vor dem eigenen Einsatz sich selbst bescheinigen und zertifizieren lassen?

Auch stellt sich die Frage, ob ein Hersteller überhaupt alle Betreiber gemäß § 9b Abs. 5 BSIG kennen und informieren kann, wenn Reseller zum Einsatz kommen oder gebrauchte kritische Komponenten weiterverkauft werden.

§ 9b Abs. 5 Nr. 5 besagt:

„Ein Hersteller einer kritischen Komponente ist nicht vertrauenswürdig, wenn […] 5. die kritische Komponente über technische Eigenschaften verfügt oder verfügt hat, die geeignet sind oder waren, missbräuchlich auf die Sicherheit, Integrität, Verfügbarkeit oder Funktionsfähigkeit der Kritischen Infrastruktur einwirken zu können.“

Das entspricht von der Formulierung auch jeder Lawful Interception-Schnittstelle. Sind diese dann in allen kritischen Komponenten nicht mehr zulässig und müssen daher konsequent unterbunden werden?

Bedeutet das dann letztlich auch, dass Vordertüren statt Backdoors, Lawful Interception-Schnittstellen und angeordnetes Ausleiten der Daten dafür sorgen, dass diese Komponenten nicht als kritische Komponenten eingesetzt werden dürften, weil es bei Schnittstellen naturgemäß immer die Möglichkeit gibt, dass darauf eingewirkt werden kann?

Insgesamt stellt die Einführung der kritischen Komponenten auch eine neue Form der Erlaubnis zum Marktzugang als auch der Marktbeschränkung dar. Wie kann daher eine langfristige Verhinderung der Monopolbildung für kritischen Komponenten sichergestellt werden?

Wenn durch die Vertrauenswürdigkeitserklärung der Kreis der Hersteller reduziert wird, wie wird sichergestellt, dass sich diese dann nicht als effektives Ziel herausstellen wie bei SolarWinds?

Wenn beispielsweise mittelfristig der einzige (Monopol) oder die einzigen beiden (Oligopol) verbleibenden Hersteller kritischer Komponenten als Single Point of Failure kompromittiert werden sollten, entstehen weitreichende Probleme großen Ausmaßes. Wurde dies angemessen berücksichtigt?

§ 9b Abs. 5 Nr. 4 BSIG besagt:

„Ein Hersteller einer kritischen Komponente ist nicht vertrauenswürdig, wenn […] 4. er bekannte oder bekannt gewordene Schwachstellen oder Manipulationen nicht unverzüglich dem Betreiber der Kritischen Infrastruktur meldet und beseitigt“

Ab dann ist der Hersteller also nicht mehr Vertrauenswürdig. Das BSI wiederum soll aber nach § 7b BSIG das Zurückhalten von Schwachstellen für den deutschen Staat vornehmen und exakt das in § 9b BSIG vorgegebene *„bekannte oder bekannt gewordene Schwachstellen oder Manipulationen nicht unverzüglich dem Betreiber der Kritischen Infrastruktur meldet und beseitigt“* unterlassen. Dies stellt einen erheblichen Wiederspruch dar.

Weiterhin stellt sich die Frage, wie die Aufrechterhaltung der kritischen Geschäftsprozesse - trotz Untersagung durch das BMI - sichergestellt werden soll. Wie kann dann die Vermeidung von Versorgungsengpässen oder -ausfällen durch die KRITIS Betreiber gewährleistet werden?

Der Gesetzesentwurf sieht ja die Untersagung oder z. B. einen Rückbau von verbauten Komponenten als Anordnung vor. Hier können also KRITIS Sektoren durch nicht durchdachte aber politisch motivierte Regulierungen lahmgelegt und die Bevölkerung unnötig gefährdet werden.

Über den Sektor IT und TK hinaus betrifft dies mindestens auch die Sektoren Energie und Wasser, da diese durch den Betrieb von Werks-Telekommunikationsnetzen ebenfalls betroffen sein werden. Ob das alles in allem daher Zweckdienlich ist, bleibt stark zu bezweifeln.

Die Regelungen in § 9b BSIG gehen weit über BSI Verantwortlichkeiten hinaus, daher wird in diesem Zusammenhang nur noch das BMI genannt, was die politische getriebene Motivation statt der Erhöhung der IT-Sicherheit auch an dieser Stelle deutlich aufzeigt.

Digitale Souveränität & der Detailgrad

Derzeit können nicht alle unter § 8a BSIG fallenden KRITIS Betreiber vollständig adressiert werden, weil einige z. B. die Anerkennung, KRITIS Betreiber zu sein, per Gerichtsstreit gegenüber dem BSI verweigern.

Darüber hinaus liegt bei anderen der Schwellenwert so niedrig, dass er wie im Sektor Wasser weniger als 50 von ca. 5.000 Wasserwerken als KRITIS Betreiber einstuft.

Weiterhin verzögern viele KRITIS Betreiber die fristgerechte Nachweiserbringung nach § 8a Abs. 3 BSIG.

Wenn dadurch also die kritischen Dienstleistungen der Versorgung mit Strom, Wasser usw. noch nicht bestmöglich nach den Vorgaben in § 8a BSIG komplett abgedeckt werden, was bringt uns dann eine Zertifizierung von kritische Komponenten und kritische Funktionen?

Wollen wir also mehr Anforderungen im Detail, weil die grundsätzliche und übergeordnete Strategie fehlt oder nicht erreicht wird? Bedeutet dies, dass das IT-SiG 1.0 bei der Zielerreichung in Teilen versagt hat, aber dies mangels Evaluierung nicht angemessen und sinnvoll nachjustiert werden kann? Soll aber dafür eine weitere sehr kontroverse Zertifizierung auf Detailebene eingeführt werden, um dies zu kaschieren?

Grundsätzlich ist alles Relevante und Wesentliche zum Schutz kritischer Infrastrukturen bereits vorhanden, nämlich die Umsetzung eines angemessenen und branchenspezifischen Stand der Technik nach § 8a BSIG. Sprich einem ISMS mit BCM. Genau dies ist daher als eines der wesentlichen Ziele des IT-SiG 2.0 zu fördern, zu intensivieren und zu verstärken.

Wo soll ansonsten die Reise nach einem Versagen der Zertifizierung von kritischen Komponenten und kritische Funktionen im nächsten Schutzschritt hinführen? In die Gesinnungsprüfung der Entwickler des Quellcodes von kritischen Komponenten?

Eine Beteiligung und Integration von Wissenschaft, Wirtschaft, Zivilgesellschaft und Sicherheitsforscher:innen ist deutlich angebracht, um den technisch-wissenschaftlichen Sinn und Unsinn solcher hochpolitischen Maßnahmen gleich aufzuzeigen und zielgerichtete Lösungsansätze zu erarbeiten, die ihre Wirkung auch erreichen können.

Digitale Souveränität & Open Source Untersagung

Durch die Anforderung einer Vertrauenswürdigkeitserklärung wird auch der Einsatz von Open Source bzw. FOSS im Bereich der kritischen Komponenten und damit bei betroffenen KRITIS Betreibern faktisch nicht mehr zulässig.

Wobei aber eben genau durch Open Source KRITIS Betreibern ermöglicht wird, kritische Komponenten länger als bei proprietärer Software üblich kontinuierlich zu Warten und zu pflegen (oder warten und pflegen zu lassen) und dadurch dauerhaft sicher zu betreiben und eben keinen Austausch vornehmen zu müssen, der ggf. einen Versorgungsengpass bei der kritischen Dienstleistung - wie der Verfügbarkeit von Strom oder Wasser - bewirkt.

EU Cyber Security Act (CSA) und freiwilliges IT-Sicherheitskennzeichen

§ 9c BSIG fordert ein freiwilliges IT-Sicherheitskennzeichen, zusätzlich zur Umsetzung des EU CSA in § 9a BSIG. Die Regelungen des § 9c BSIG sind dabei allerdings im Kern deckungsgleich mit den in § 9a BSIG geregelten Sachverhalte.

Ein freiwilliges IT-Sicherheitskennzeichen einzuführen doppelt sich mit der in § 9a BSIG erforderlichen Umsetzung des EU CSA, denn dieser behandelt bereits alle erforderlichen Aspekte zu Zertifizierungen, welche sich auch auf Consumer Devices erstrecken können.

Nutzer:innen von Consumer Devices lassen sich sehr grob in zwei Kategorien einteilen.

Zum einen in technik- und sicherheitsaffine Menschen, die ein IT-Sicherheitskennzeichen nicht benötigen und sich selber sachkundig informieren können und daher ohne das Kennzeichen informieren werden.

Und zum anderen in alle anderen Menschen, welche im Wesentlichen schon beim Scan eines QR-Codes mit dem Smartphone überfordert sein werden und darüber hinaus ein solches Kennzeichen nicht als solches erkennen können, geschweige denn richtig interpretieren werden. Darüber hinaus werden diese Nutzer:innen auch mit einem solchen Kennzeichen weder was anfangen können, noch ein gesteigertes Interesse an Sicherheitsinformationen haben, welche sie erst über den Umweg der Nutzung einer Technologie - und nur dann - angezeigt bekommen.

Ein freiwilliges IT-Sicherheitskennzeichen ist dafür aber sicherlich für Marketing- und Vertriebsverantwortliche bei Herstellerfirmen eine interessante Option. Aus dieser Position heraus könnte das Produktionsteam gefragt werden, wie lange ein Produkt, das aktiv vermarktet werden soll, mit Sicherheitspatches versorgt werden soll. Und genau für den Zeitraum würde das freiwillige IT-Sicherheitskennzeichen aktiv eingesetzt und vermarktet werden.

Kurz vor Ablauf der Versorgung mit Sicherheitspatches könnte das freiwillige IT-Sicherheitskennzeichen entfernt bzw. für genau dieses Produkt aufgekündigt werden. Damit steht selbst ein mittelmäßiger bis schlechter Hersteller gut da und hätte ein Produkt im Portfolio (gehabt), welches für den Hauptzeitraum am Markt mit einer zugelassenen und vom BSI amtlich wirkenden „Sicherheitsprüfung“ beworben wird. Hersteller, die kein Interesse an Sicherheit haben, werden das freiwillige IT-Sicherheitskennzeichen schlicht ignorieren, da kein Marktdruck durch den Wettbewerb zu erwarten ist.

Davon abgesehen ist eine Selbstauskunft auf Dokumentenbasis bereits ausreichend, das freiwillige IT-Sicherheitskennzeichen zu erhalten. Eine technische Prüfung eines Sachkundigen oder sogar eines unabhängigen Dritten ist dabei nicht vorgesehen.

Auch hier stellt sich wieder die Frage, ob bedingt durch diese zukünftig vorgesehenen Zertifizierungen und Konformitätsbewertungen nach § 9a BSIG oder § 9c BSIG Open Source und FOSS benachteiligt wird.

Es wird daher empfohlen, den § 9c BSIG ersatzlos zu streichen und die unnötige Bindung von Personal und weiteren Ressourcen hierdurch zu vermeiden.

Sanktionen & (nicht vorhandene) Incentivierungen

In § 14a BSIG muss das BSI für Institutionen der sozialen Sicherung aufgrund des Einvernehmens mit den zuständigen Aufsichtsbehörden mögliche Sanktionen von diesen bestätigen lassen. Die Aufsichtsbehörden sollen grundsätzlich geeignete Durchsetzungsmittel zur Verfügung stellen können, welche im Falle des Falles auch bedeuten, Zwangsmittel androhen können. Diese Zwangsmittel wären aber in jedem Fall günstiger als nur eine Maßnahme zur Informationssicherheit umzusetzen.

Durch seine Vorbildfunktion sollte der Staat sich und seine Behörden - in diesem Fall die Institutionen der sozialen Sicherung - nicht von Sanktionen ausnehmen. Eine Sonderstellung kann an dieser Stelle weder als vertrauensfördernd noch als Erhöhung der IT-Sicherheit verstanden werden und ist daher ersatzlos zu streichen.

Weiterhin stellt sich die Frage, ob auch zusätzlich zur Erweiterung der Sanktionierungsmaßnahmen eine Incentivierung und somit positive Motivation zur Erhöhung der IT-Sicherheit hinreichende Berücksichtigung gefunden hat. Wurden Möglichkeiten dieser Option nicht evaluiert oder in Betracht gezogen?

So könnten beispielsweise Unternehmen, die ein ISMS mit BCM aufsetzen und zertifizieren, diese Betriebsausgaben für ihre IT-Systeme steuermindernd geltend machen. Dies wird mittel- bis langfristig dazu führen, dass IT-Sicherheit durch den im ISMS vorgesehenen iterativen Prozess zum Lernen und zur Verbesserung der Sicherheitsmaßnahmen gemäß Demingkreis[16] kontinuierlich gesteigert wird.

Ausstehende Evaluierung des IT-SiG 1.0

Inzwischen liegen sechs Jahre zwischen dem ersten IT-SiG (2015) und der aktuellen Gesetzesfassung des IT-SiG 2.0 (2021). Daher müsste man eigentlich davon ausgehen können, dass das in die Wege gebrachte Gesetz zunächst in seiner Wirkung evaluiert und der Gesetzgeber dann die vorgesehenen Nachbesserungen damit begründet. Und um genau diese Vorgehensweise sicherzustellen, wurde im IT-SiG 1.0[17] sogar eine Evaluierung in Artikel 10 „Evaluierung“ rechtlich vorgeschrieben.

[16] https://de.wikipedia.org/wiki/Demingkreis

[17] https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl115s1324.pdf#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl115s1324.pdf%27%5D__1614281214462

Hierbei ist bereits nach vier Jahren *„unter Einbeziehung eines wissenschaftlichen Sachverständigen, der im Einvernehmen mit dem Deutschen Bundestag bestellt wird, zu evaluieren“*.

Die immer noch ausstehende aber gesetzlich vorgegebene Evaluierung der Wirksamkeit der aktuellen Gesetzesfassung sorgt weiterhin dafür, dass die Gesetzesbegründung und Kritiken daran mangels Evidenz-Erhebung an vielen Stellen einer gesicherten Erkenntnisgrundlage entbehren.

Das IT-SiG 2.0 enthält auf den ersten Blick zwar einige sinnvolle Regelungsansätze, viele der Neuerungen scheinen aber noch nicht zu Ende gedacht. Auch die erheblichen Kritiken seit dem ersten öffentlich gewordenen Entwurf des IT-SiG 2.0 aus 2019 sind beim Gesetzgeber bisher offenbar weitestgehend stumm verklungen. Eine Evaluierung der bereits bestehenden gesetzlichen Maßnahmen ist daher vor diesem Hintergrund nicht nur wünschenswerter denn je, sondern Voraussetzung für die Zielerreichung einer Erhöhung der IT-Sicherheit in Deutschland.

Daher verwundert es doch sehr, dass immer noch an der Einführung des IT-SiG 2.0 geklammert wird, ohne dass eine vollständige Evaluierung des IT-SiG 1.0 abschließend vorgenommen wurde. Es stellt sich daher die Frage, wieso der Gesetzgeber eine Gesetzesüberabreitung und -erweiterung vornimmt, wenn das bisherige nicht evaluiert wurde.

Eine entsprechende Anfrage zur „Evaluierung IT Sicherheitsgesetz“ über FragDenStaat[18] wurde im Oktober 2019 vom BMI damit ablehnend begründet, dass die BSI-Kritisverordnung (BSI-KritisV) *„am 03. Mai 2016 erstmals in Kraft getreten“* sei.

Vier Jahre später gab es aber immer noch keine Evaluierung.

Eine erneute Anfrage[19] ergab dann einen plötzlich folgenden Sinneswandel zur Auslegung einer Begründung für eine erneute Verzögerung:

„Im Hinblick auf die Sektoren Finanzen, Transport und Verkehr sowie Gesundheit wurde die BSI-KritisV erst mit Inkrafttreten des zweiten Korbs am 30. Juni 2017 vervollständigt.“

Nach dieser neuen - zugegebenermaßen sehr kreativen Rechenart des BMI zur zuletzt gültigen Version der BSI-KritisV - würde die Evaluierung erst zum 30. Juni 2021 fällig werden. Allerdings wird mindestens durch die Einführung des neuen KRITIS Sektors Siedlungsabfallentsorgung eine neue BSI-KritisV fällig werden und sich die Evaluierung erneut um vier Jahre verschieben können.

Des Weiteren würde mit der im IT-SiG 2.0 beschriebenen Neuregelung der Evaluierung in Artikel 6 selbige zeitlich sogar noch weiter nach hinten geschoben. Es soll zudem keine Evaluierung des für KRITIS wesentlichen Anwendungsbereichs der §§ 8a und 8b BSIG erfolgen, denn gemäß Artikel 6 Abs. 2 wird vorgesehen, dass *„Artikel 10 des Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme vom 17. Juli 2015 (BGBl. I S. 1324)“* ersatzlos aufgehoben wird.

Dies würde aktuell daher auch bedeuten, dass keine IT-SiG 1.0 Evaluierung mehr vorzunehmen ist. Dadurch bleiben alle im IT-SiG 1.0 vorgenommenen Regelungen von 2015 bis 2021 außen vor!

Daher ist Artikel 6 Abs. 2 zu streichen und umgehend zu evaluieren, was die §§ 8a und 8b BSIG gebracht haben, da diese ja kaum verändert werden, aber im ersten IT-SiG eingeführt wurden und jetzt hätten evaluiert werden müssen.

[18] https://fragdenstaat.de/anfrage/evaluierung-it-sicherheitsgesetz/
[19] https://fragdenstaat.de/anfrage/evaluierung-it-sicherheitsgesetz-1/

Ansonsten würden diese grundsätzlichen Regelungen zum Kern Kritischer Infrastrukturen erst zwei Jahre später evaluiert werden, sprich in 2023. Lernkurven oder „Lessons Learned“ lassen sich so in jeglicher Form sträflich missen. Es erweckt daher eher den Anschein, als wolle der Gesetzgeber bei der Versorgungssicherheit der Bevölkerung durch kritische Infrastrukturen nach „Trial and Error“ Methode[20] verfahren.

Durch die fehlende Evaluierung kann nicht nachvollzogen werden, ob z. B. die aktuellen Schwellenwerte die vorgegebenen Schutzziele erreichen oder daran vorbei schlittern und Risiken zur Gefährdung der Versorgungssicherheit angemessen adressiert werden. Drei Beispiele hierzu:

- Im Sektor Wasser sind lediglich unter 50 von ca. 5.000 Wasserwerken KRITIS Betreiber. Reicht dies aus? Wenn ja, warum?
- Sektorübergreifende KRITIS Betreiber und die damit verbundenen kumulierenden Risiken - z. B. bei kommunalen Energie- und Wasserwerksbetreibern einschließlich öffentlichem Transport & Verkehr - wurden bisher nicht betrachtet. Ist das nicht relevant? Wenn nicht, warum?
- Wechselwirkungen und Abhängigkeiten von KRITIS Betreibern untereinander – z. B. die Abhängigkeit von Strom und Wasser bei einem KRITIS Betreiber aus einem anderen Sektor - wurden nicht berücksichtigt. Ist das nicht relevant? Wenn nicht, warum?

Auch fehlende Befugnisse für das BSI und Defizite in den Vorgaben durch das BSI wurden offenbar nicht evaluiert und im Gesetzesentwurf berücksichtigt. Dieser wurde daher inzwischen durch die Realität eingeholt. Hier ein Auszug von inzwischen offensichtlichen Fragestellungen im genannten Zusammenhang:

- Wieso haben immer noch nicht alle KRITIS Betreiber ein vernünftiges ISMS mit BCM implementiert und leben dieses aktiv im Betrieb?
- Wieso gibt es Prüfer, die nicht ordentlich und angemessen Prüfen oder ausreichende Fachkenntnisse nachweisen können?
- Wieso gibt es keine sog. Mockup Audits der Prüfer und keine Akkreditierung der Prüfenden Stellen KRITIS?
- Wieso gibt es kein definiertes Prüfverfahren wie beim IT-Grundschutz?
- Wieso haben viele KRITIS relevante Informationen des BSI nur empfehlenden Charakter in Form von Orientierungshilfen und sind daher nicht verbindlich oder gesetzlich bindend?
- Wieso kann jeder Schulungsanbieter die „zusätzliche Prüfverfahrenskompetenz für § 8a BSIG“ für KRITIS Prüfer beliebig gestalten?
  Beispielsweise mit oder ohne Prüfung, ein oder zwei Tage, vor Ort bzw. persönlich oder aufgezeichnete Websession.

Vorhandene Defizite in den Kompetenzen der KRITIS Prüfer als auch in der Qualität der Durchführung von KRITIS Prüfungen sollte das BSI mittels konkreter und verbindlich einzuhaltender Vorgaben in § 8a Abs. 5 BSIG gegensteuern. Und darüber hinaus diese auch regelmäßig selber prüfen, beispielsweise durch Mockup-Audits der einzelnen KRITIS Prüfer und durch eine verbindlich

[20] https://de.wikipedia.org/wiki/Versuch_und_Irrtum

vorgegebene und formale Akkreditierung der Prüfenden Stellen, in der Art vergleichbar wie beim IT-Grundschutz.

Die implizite Formulierung in § 8a BSIG ergibt, dass ein ISMS mit BCM zu betreiben ist, was auch das BSI erwartet. Dies wird allerdings nicht explizit in diesem Paragraphen erwähnt. Dies wäre ebenfalls ein Beispiel, einen Teil der erwähnten Defizite aufzulösen, den Gesetzestext für Betroffene lesbarer zu gestalten und den Diskussionen hierzu durch Klarstellung im Gesetzestext Einhalt zu gebieten.

Die ausstehende Evaluierung ist daher unverzüglich in die Wege zu leiten und die daraus gewonnenen Erkenntnisse vor Verabschiedung des IT-SiG 2.0 zwingend in dieses einzuarbeiten. Die Ergebnisse der Evaluierung sollten dabei abstrakt öffentlich gemacht werden, damit Transparenz geschaffen wird, ob und welche Ziele erreicht wurden.

In Artikel 6 ist daher darüber hinaus vorzusehen, dass die Evaluierung nicht nur in Teilen, sondern vollumfänglich und darüber hinaus auch nach wissenschaftlichen Standards durch eine unabhängige Stelle zu erfolgen hat. Die Ergebnisse sind auf der Homepage des BMI zu veröffentlichen.

Gestrichene Themen und Optimierungspotential

Im Entwurf von Mai 2020 waren die Krisenreaktionspläne noch vorhanden und wurden positiv begrüßt. Das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) sollte im zuvor enthaltenen § 5c BSIG wichtige Aufgaben und weitere Personalstellen zugeteilt bekommen, um erstmalig in die Lage versetzt zu werden, auch für IT-Katastrophen Krisenreaktionspläne auszuarbeiten. Auch wäre der neu geschaffene § 5c BSIG fast schon wie die initiale rechtliche Grundlage für den Einsatz eines zu schaffenden Cyber-Hilfswerks[21] - wie von der AG KRITIS im Februar 2020 auf der DefensiveCon[22] erstmalig öffentlich vorgestellt[23] - und verortet die Kompetenzen und Verantwortlichkeiten an den richtigen Stellen, nämlich dem BSI gemeinsam mit dem Partner BBK.

Dieser Paragraph ist leider ersatzlos gestrichen worden - obwohl Krisenreaktionspläne als auch ein Zuwachs beim BBK dringend notwendig sind. Resilienz erfordert auch die Fähigkeit, auf Krisen angemessen reagieren zu können - nur mit einer Mehrausstattung von BMI und Cyber-Kräften kann diesem nicht genüge getan werden. Es erfordert daher zusätzliche Stellen beim BBK, was sich gerade in diesen Zeiten der Pandemie klarer als je zuvor darstellt und auf der Hand liegt.

Viele der Branchenspezifischen Sicherheitsstandards (B3S)[24] sind nicht öffentlich verfügbar. Wieso sind B3S nicht verpflichtend auf der BSI Webseite zu veröffentlichen und freizustellen, damit der angemessene und branchenspezifische Stand der Technik eingesehen und transparent dargestellt

[21] https://ag.kritis.info/chw-konzept/
[22] https://www.defensivecon.org
[23] https://media.ccc.de/v/dcon2020-18-cyberhilfswerk-konzeption-fr-eine-cyberwehr-2-0
[24] https://www.bsi.bund.de/DE/Themen/KRITIS-und-regulierte-Unternehmen/Kritische-Infrastrukturen/Allgemeine-Infos-zu-KRITIS/Stand-der-Technik-umsetzen/Uebersicht-der-B3S/uebersicht-der-b3s_node.html

werden kann? Eine Verpflichtung zur Veröffentlichung, um ein Peer Review des in den B3S enthaltenen Stand der Technik zu erreichen und diesen öffentlich zu diskutieren erscheint daher zielführend im Sinne des Gesetzes.

Um diese Peer Reviews für den Stand der Technik zu ermöglichen ist als Vorgabe im Verfahren nach § 8a Abs. 2 BSIG vorzugeben, dass ein B3S nach erfolgreich vorgenommener Eignungsfeststellung auf der Webseite des BSI zu veröffentlichen ist.

Der Stand der Technik wird im Handbuch der Rechtsförmlichkeit[25] beschrieben und definiert.

In § 3 Abs. 20 BSIG wird die *„Entwicklung und Veröffentlichung eines Stands der Technik bei sicherheitstechnischen Anforderungen an IT-Produkte."* durch das BSI beschrieben. An dieser Stelle sollte besser die vorherige verwendete Formulierung verwendet werden: *„Entwicklung und Veröffentlichung sicherheitstechnischer Anforderungen an IT-Produkte."*, da der Stand der Technik nicht von einer Stelle festgelegt, sondern von der herrschenden Mehrheit der Fachexperten wie z. B. Fachgremien gefestigt wird.

Als negatives Beispiel seien hier die Passwortrichtlinien im IT-Grundschutz angegeben, wo das BSI mit seinem bis letztes Jahr gültigen regelmäßigen Passwortwechsel recht alleine auf weiter Flur stand, da alle anderen maßgeblichen Sicherheitsstandards schon die Formulierungen auf den neueren und allgemein anerkannten Stand der Technik umgestellt hatten.

Symptomatisch handlungsunfähig im Cyberraum

Das ganze IT-SiG 2.0 ist leider symptomatisch dafür, wie unsystematisch das Thema Informationssicherheit in Deutschland betrieben wird.

Das zeigt sich schon an der langen Liste staatlicher Akteure in der Cybersicherheitsarchitektur Deutschlands alleine auf Bundesebene, die in der Übersicht der SNV[26] regelmäßig erweitert werden muss.

Es zeigt sich aber auch in der Cybersicherheitsstrategie Deutschlands 2016, die ausschließlich BMI Zuständigkeiten widerspiegelt, als ob Deutschland nur aus den vom BMI verantworteten Bereichen besteht. Die Frage nach der digitalen Souveränität muss sich Deutschland daher gar nicht erst stellen, die Antwort liegt auf der Hand. Oder besser gesagt in der Hand… des BMI.

Ein übergreifendes strategisches Konzept, dass auch Länder, Kommunen, Wissenschaft & Forschung, Bildung, Wirtschaft, Zivilgesellschaft und Sicherheitsforscher:innen sinnvoll einbettet, fehlt völlig.

Hier wurde erneut die Chance vertan, das BSI ordentlich als zentrale Stelle zur Vernetzung all dieser weiteren Akteure möglichst unabhängig aufzustellen und in dieser Rolle zu stärken. Stattdessen wird es zu Teilen zum Handlanger oder verlängerten Arm von Sicherheitsbehörden und Nachrichtendiensten.

---

25 https://www.bmjv.de/SharedDocs/Downloads/DE/Themen/RechtsdurchsetzungUndBuerokratieabbau/HandbuchDerRechtsfoermlichkeit_deu.pdf?__blob=publicationFile&v=2

26 https://www.stiftung-nv.de/sites/default/files/snv_papier_cybersicherheitsarchitektur_final.pdf

Die Regelung der Zusammenarbeit der staatlichen Stellen, z.B. im Cyber-Abwehrzentrum wird auch weiterhin nicht auf eine ordentliche gesetzliche Grundlage gestellt. Dies ist längst überfällig, da sich dort inzwischen eine Vielzahl von Behörden ohne jede transparente Regelung austauschen. Das Trennungsgebot von Polizei und Nachrichtendiensten wird dadurch unterlaufen.

Auch der aktuelle Entwurf löst das Problem von mehrfachen Behördenzuständigkeiten nicht auf. So müssen Meldungen nach § 109 TKG weiterhin sowohl an das BSI als auch an die Bundesnetzagentur erfolgen. Das erzeugt bei den Betreibern Mehraufwände, ohne dass dem ein Mehrwert gegenübersteht. Warum die im IT-Sicherheitsgesetz von 2015 noch vorgesehene Weitergabe der Meldung von einer Behörde an die andere nicht ausreicht, ist unklar.

Die Kostenschätzung für die Wirtschaft ist eher kreativ plump ausgefallen als transparent und nachvollziehbar. Der Aufwand für die Wirtschaft ist deutlich zu niedrig geschätzt worden. Das Jahresgehalt einer gut ausgebildeten IT-Sicherheitsfachfrau liegt laut Mineralölwirtschaftsverband e.V. (MWV) bei etwa 80.000 € zzgl. Sozialabgaben. Der MWV stellt unter anderem durch detailliertere Kostenaufstellungen in seiner Stellungnahme[27] dar, dass die Berechnungen des BMI haltlos und viel zu niedrig angesetzt sind.

Das gleiche gilt für die Kostenschätzungen für Angriffserkennungssysteme nach § 8a Abs. 1a BSIG. Mit dem Betrieb, der Hard- und Software einschließlich Lizenzgebühren, dem Personal und den zugehörigen Prozessen sind diese durchaus deutlich teurer anzusetzen. Der Erfüllungsaufwand für die Wirtschaft ist daher insgesamt nicht nachvollziehbar beziffert.

In diesem Zusammenhang ist auch festzustellen, dass es unsinnig ist, dass bestimmte Einzelmaßnahmen wie Angriffserkennungssysteme explizit als neue Regelung im Gesetz eingeführt werden sollen. Denn welche konkreten Maßnahmen zur Absicherung ergriffen werden müssen, ergibt sich aus einer Risikoanalyse im Rahmen des ISMS mit BCM nach § 8a BSIG.

Wenn Angriffserkennungsmaßnahmen durch die explizite Nennung im Gesetzestext entsprechende Priorität einzuräumen ist, fehlen die dafür aufzuwendenden Ressourcen im Zweifel bei den Maßnahmen, die nach der Risikoanalyse wichtiger und dringend nötiger sind, z. B. eine angemessen abgesicherte Fernwartung nach Stand der Technik, wie sie im Wasserwerk in Texas[28] nicht vorhanden war. Auch in Deutschland sind aktuell solche Szenarien im Betrieb via Fernwartung weiterhin Alltag.

Diese Neuregelung ist auch deswegen nicht nachvollziehbar, weil Angriffserkennungssysteme auch bisher schon zu den technischen Maßnahmen zählen, die nach § 8a Abs. 1 BSIG umzusetzen sind. In der Gesetzesbegründung zum IT-Sicherheitsgesetz 2015 werden solche Detektionsmaßnahmen explizit als Teil der Pflichten nach § 8a Abs. 1 BSIG genannt. [29]

Auch im KRITIS-Sektor Staat und Verwaltung gibt es noch deutliches Verbesserungspotential. Es ist erfreulich zu sehen, dass mit § 4a BSIG und § 8 BSIG auch neue Regelungen für den Bereich der Bundesbehörden eingeführt werden. Diese reichen in der derzeitigen Form allerdings nicht aus. Es ist

[27] https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/entwurf-zweites-it-sicherheitsgesetz.html
[28] https://www.lebensraumwasser.com/hackerangriff-auf-wasserwerk-in-den-usa/
[29] BT-Drucksache 18/4096, Seite 25

nicht nachvollziehbar, warum wichtige und wesentliche Bereiche wie das Auswärtige Amt oder weite Teile des BMVg ausgenommen sind. Dass an diesen Stellen eine Kontrolle durch eine zentrale Stelle sinnvoll ist, hat der Angriff auf das Auswärtige Amt medienwirksam belegt.

Auch im Bereich der KRITIS-Prüfungen von KRITIS Betreibern ist daher richtigerweise eine unabhängige Prüfung der ergriffenen IT-Sicherheitsmaßnahmen durch § 8a Abs. 3 BSIG und Nr. 1.4.2. der Orientierungshilfe des BSI[30] vorgesehen.

Warum für den Sektor Staat und Verwaltung in Teilen von diesem Grundsatz abgewichen werden soll, ist daher absolut unverständlich.

Ebenfalls fragwürdig ist es, dass das BSI die einzuhaltenden Mindeststandards für die Bundesverwaltung nach § 8 Abs. 1 BSIG nur im Einvernehmen mit den anderen Ressorts festlegen kann. Diese werden sich - anders als das BSI - bei der Frage im Zweifel nicht nur an den Erfordernissen der IT-Sicherheit orientieren. Sie werden sich wohl eher davon leiten lassen, den eigenen Aufwand für die Umsetzung möglichst gering zu halten. Im Sinne der IT-Sicherheit ist es daher erforderlich, dass die Mindeststandards vom BSI festgelegt werden.

Dabei muss das BSI die Positionen der Ressorts sicherlich berücksichtigen. Das richtige Instrument dafür ist daher die Herstellung des Benehmens. Schon beim ersten IT-Sicherheitsgesetz 2015 wurde daher für § 8 Abs. 1 BSIG das Einvernehmen durch das Benehmen ersetzt. Warum das jetzt geändert werden soll, ist nicht nachvollziehbar.

Bei den Krisenbewältigungsaufgaben des BSI ist nicht nachvollziehbar, warum das BSI nach dem neuen § 8b Abs. 4a BSIG im Fall einer erheblichen Störung zur Herausgabe von Informationen das Einvernehmen mit der für den jeweiligen Betreiber zuständigen Aufsichtsbehörde suchen muss. Die Bewältigung der Störung muss hier Priorität gegenüber den Befindlichkeiten der zuständigen Aufsichtsbehörde haben. Es würde daher vollkommen ausreichen, die zuständige Aufsichtsbehörde in Kenntnis zu setzen. Dieses Detail zeigt erneut einen groben handwerklichen Fehler, der die Bewältigung einer erheblichen Störung unnötig verzögert. Dieses Einvernehmenserfordernis ist daher aus § 8b Abs. 4a BSIG zu streichen.

Es muss sich auch die Frage gestellt werden, ob das BSI wirklich alleine in der Lage ist, alle neuen Aufgaben im Bereich der Cybersicherheit zu übernehmen. Mit jeder neuen Aufgabe besteht die Gefahr, dass das BSI zwar neue Aufgaben bekommt, diese aber nicht alle erfüllen können wird. So kann man z. B. das BSI Mobile Incident Response Team sicherlich weiter ausbauen, aber zur Bewältigung drohender Cyber-Großschadenslagen mit vielen Betroffenen in ganz Deutschland werden sie trotzdem nie ausreichen können. Die Wahrscheinlichkeit einer solchen Cyber-Großschadenslage steigt aber durch die fortschreitende Digitalisierung - auch in der Prozessautomatisierung - kontinuierlich und stetig an.

[30] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Kritis/Orientierungshilfe_8a_3_v11.pdf

Daher sollte an einem Gesamtkonzept für die Cybersicherheit in Deutschland gearbeitet werden, welches auch die Einbettung des von der AG KRITIS konzipierten Cyber-Hilfswerk[31] zur Unterstützung mittels ehrenamtlich tätiger Expert:innen Berücksichtigung findet.

Fazit

Der Gesetzesentwurf zum IT-SiG 2.0 stellt in seiner aktuellen Form ein strategieloses Bürokratiemonster dar, welches der Anforderung zur Erhöhung der IT-Sicherheit nicht gerecht wird.

Die Cybersicherheit und die digitalen Souveränität Deutschlands bleiben dabei auf der Strecke.

Auch und insbesondere, dass in diesem Gesetzesentwurf keine Alternative unter Punkt C angegeben wird, lässt tief blicken. Es ist schlichtweg nicht nachvollziehbar, dass bei solch umfassenden Zielvorgaben keine einzige Alternative benannt wird. Dies ist sicherlich insbesondere auf die fehlende Evaluierung der Effektivität aller im IT-SiG 1.0 vorgegebenen Maßnahmen zur Erhöhung der Sicherheit informationstechnischer Systeme zurückzuführen.

Viele Alternativen wurden trotz alledem in dieser Stellungnahme aufgezeigt und finden hoffentlich ihren konstruktiven Weg in den Gesetzesentwurf, um nichts weniger als die Cybersicherheit zum Schutz der Zivilgesellschaft zu gewährleisten.

Die AG KRITIS steht hierfür gerne weiterhin ehrenamtlich beratend für den Gesetzgeber und die demokratischen Parteien zur Verfügung.

[31] https://ag.kritis.info/chw-konzept/

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
19(4)741 D

Stellungnahme zu der Anhörung

Vorlagen zur IT-Sicherheit

des Ausschusses für Inneres und Heimat des Deutschen Bundestages am 1. März 2021

Martin Schallbruch, Digital Society Institute, ESMT Berlin
26. Februar 2021

0. Zusammenfassung

Angesichts der dramatisch verschlechterten Cybersicherheitslage (Abschnitt 1) ist die Weiterentwicklung des IT-Sicherheitsrechts durch das IT-Sicherheitsgesetz 2.0 zu begrüßen. Die geplanten gesetzlichen Regelungen bewegen sich in einem sehr dynamischen nationalen und europäischen Regulierungsumfeld (Abschnitt 2). Der vorliegende Gesetzentwurf der Bundesregierung entwickelt das IT-Sicherheitsgesetz grundsätzlich sinnvoll weiter. Eine vor allem auf Befugniserweiterung des BSI setzende Strategie wird dem Schutzbedarf der deutschen Wirtschaft allerdings nicht ausreichend gerecht (Abschnitt 3). Wesentliche Defizite des Entwurfs können durch einzelne Änderungen beim Schutz des Bundes, der Einbeziehung weiterer Unternehmen, der Produktsicherheit und der Technikregulierung behoben werden (Abschnitt 4). Weitergehende Gesetzgebungsbedarfe bei der aktiven Cyberabwehr, der Cybersicherheitsarchitektur, dem Umgang mit Schwachstellen und der Systematisierung des IT-Sicherheitsrechts sollten in der kommenden Wahlperiode aufgegriffen werden (Abschnitt 5).

1. Zur Lage der IT- und Cybersicherheit

Die Lage der IT- und Cybersicherheit hat sich in den vergangenen Jahren besorgniserregend verschlechtert.

Das vom Bundeskriminalamt (BKA) im September 2020 veröffentlichte Bundeslagebild Cybercrime verzeichnet einen Anstieg aller Delikte dieses Kriminalitätsbereichs gegenüber dem Vorjahreszeitraum um 15,4 Prozent. Gleichzeitig geht das BKA von einem weit überdurchschnittlichen Dunkelfeld in diesem Kriminalitätsbereich aus. Die Entwicklung des Cybercrime ist durch eine wachsende Professionalität der Kriminellen, eine globale Vernetzung der Täterinnen und Täter sowie ein ausgesprochen arbeitsteiliges Vorgehen im Stil einer „Underground Economy“ geprägt. Opfer von Cybercrime sind Nutzerinnen und Nutzer des Internets und zunehmend auch kleine und große Unternehmen. Zwar sind deutliche Fortschritte der

Sicherheitsbehörden bei der Bekämpfung von Cybercrime zu verzeichnen, etwa die jüngst erfolgte Übernahme der Infrastruktur von Emotet. Die verstärkten Strafverfolgungsmaßnahmen haben es aber bislang nicht vermocht, die Tendenz zu brechen.

Gleichzeitig zeigt der im November 2020 veröffentlichte jüngste Lagebericht des Bundesamtes für Sicherheit in der Informationstechnik (BSI) eine auch aus technischem Blickwinkel weiter verschärfte Gefährdungslage. Während Cyber-Angreifer immer höher entwickelte Werkzeuge und Angriffsmethoden einsetzen und weitere Gruppen von Angreifern in Deutschland aktiv sind, verzeichnet das Amt eine gleichbleibend hohe Zahl von Schwachstellen in Software- und Hardwareprodukten, darunter auch kritische Schwachstellen, die für Angriffe ausgenutzt werden. Nach wie vor sind sowohl die Produktsicherheit von Hardware und Software unzureichend als auch die Maßnahmen von IT-Betreibern zum Absichern ihrer Systeme. Schwachstellen werden teilweise über längere Zeiträume von den Herstellern oder Betreibern der Systeme nicht behoben bzw. abgesichert. Millionen von Kundendatensätzen sind über entsprechende Angriffe abgeflossen, darunter sensible Patientendaten. Gleichzeitig stieg auch die Anzahl der auf IT-Angriffe zurückzuführenden Meldungen aus dem Bereich der Kritischen Infrastrukturen an das BSI über den Zeitraum eines Jahres erheblich (von 252 Meldungen in 2018/2019 auf 419 Meldungen in 2019/2020). Auch die Bundesverwaltung ist seit 2015 in mehreren Fällen Ziel schwerwiegender Cyberangriffe geworden, vor allem auch mit nachrichtendienstlichem Hintergrund.

Die Tendenz der Berichte hat sich in den letzten 5 Jahren nicht verändert. Unternehmen und öffentlichen Einrichtungen in Deutschland ist es bislang nicht flächendeckend gelungen, einen ausreichenden Schutz ihrer Systeme gegen Cyberangriffe zu etablieren. Zwar sind bei vielen Unternehmen und auch im Behördenumfeld erhebliche Anstrengungen zu verzeichnen, ihre IT-Sicherheitsmaßnahmen, ihre Resilienz gegen Cyberangriffe und die Notfallvorsorge zu verbessern. Der nachhaltige Erfolg dieser Bemühungen wird jedoch abgeschwächt durch die steigende Komplexität der digitalen Systeme einerseits und unsere wachsende Abhängigkeit von ihrer Funktionsfähigkeit andererseits.

Mit der Virtualisierung eines Großteils der IT-Anwendungen, d.h. der Verlagerung von Anwendungen in die Cloud, mit der schnellen Verbreitung von intelligenten vernetzten Geräten (IoT) und mit dem zunehmenden Einsatz von KI-basierten Verfahren nimmt die Komplexität der IT-Systeme von Unternehmen und Behörden und damit die Komplexität der Digitalisierung ganzer Lebensbereiche zu. Dies gilt beispielsweise für das Gesundheitswesen, den Mobilitätsbereich oder auch die produzierende Wirtschaft. Das Zusammenwirken der IT-Systeme und ihre Abhängigkeit voneinander, damit letztlich auch die Sicherheit der vernetzten „digitalen Landschaft“ ist immer schwieriger zu beurteilen.

Daher sind Maßnahmen zur Verbesserung der Produktsicherheit einschließlich der Sicherheit und Vertrauenswürdigkeit entlang der gesamten Lieferkette von besonderer Bedeutung. Komplexe digitale Systeme wie eine digital gesteuerte Produktionsanlage werden aus Komponenten unterschiedlicher Hersteller aus verschiedensten Ländern gestaltet. Die Sicherheit jeder einzelnen Komponente ist grundsätzlich geeignet, die Sicherheit des Gesamtsystems zu beeinträchtigen. Der Aufwand für eine angemessene Absicherung eines solchen komplexen Systems nimmt kontinuierlich zu.

Die steigende Komplexität der Systeme wird begleitet durch eine wachsende Abhängigkeit aller Lebensbereiche von dem Funktionieren der IT- und Kommunikationssysteme. In vielen kritischen Infrastrukturen – und darüber hinaus – ist ein Weiterbetrieb der wesentlichen Leistungen bei Ausfall der IT-Systeme nicht mehr möglich. Auch kleine und mittlere Unternehmen sind in ihrer Arbeitsfähigkeit überwiegend stark von IT-Systemen abhängig, ohne dass dort ein vergleichbarer Aufwand für ihre Absicherung möglich wäre wie bei großen Konzernen. Zudem sind auch die Bürgerinnen und Bürger beim Homeschooling und Homeoffice, in ihrer privaten Lebens- und Freizeitgestaltung von funktionsfähigen und vertrauenswürdigen digitalen Geräten abhängig. Die Verletzlichkeit der digitalen Welt ist in den letzten Jahren stark gestiegen, die potentiellen Schäden durch unsichere Informationstechnik und Cyberangriffe nehmen für Unternehmen, Behörden und jede/n Einzelne/n auch aufgrund der gewachsenen Abhängigkeit zu.

Angesichts der Vielfalt der Systeme und der Dynamik der Gefährdungslage erfordert ein wirksamer Schutz ein enges und vertrauensvolles Zusammenwirken verschiedener Akteure: sowohl innerhalb der Wirtschaft als auch zwischen Staat und Wirtschaft müssen belastbare Informationsplattformen, Austausch- und Koordinierungsformate bestehen, die der wechselseitigen Unterrichtung über Schwachstellen, Angriffsformen und Schutzmechanismen ebenso dienen wie der Abstimmung von Sicherheitsmaßnahmen.

Die Beherrschung des Cyberraums ist mittlerweile ein Gegenstand der geopolitischen Auseinandersetzung. Staaten wie Russland nutzen nach Erkenntnissen des Bundesamtes für Verfassungsschutz (BfV) Cyberangriffe als nachrichtendienstliche Instrumente zur Informationsbeschaffung, Desinformation und Propaganda. Deutschland und andere EU-Staaten sind in den letzten Jahren mehrfach Opfer mutmaßlich russischer Cyberangriffe geworden. Die Volksrepublik China strebt eine weltweite Führungsrolle in der Beherrschung digitaler Technologien an. Cyberangriffe durch chinesische Nachrichtendienste – auch auf Ziele in Deutschland – sind ebenso ein Teil dieser Strategie wie die enge Kooperation zwischen chinesischem Staat und chinesischen Unternehmen zwecks weltweiter Verbreitung chinesischer Technologie. Gerade der Bereich der Infrastrukturen ist hierbei ein prioritäres Ziel.

Die Gewährleistung von IT- und Cybersicherheit in Deutschland ist insofern auf das engste verknüpft mit der sicherheitspolitischen Strategie Deutschlands, der EU und der NATO, sowie mit einer Industriepolitik der digitalen Souveränität, die sicherstellt, das auch langfristig vertrauenswürdige Technologien für Deutschland zur Verfügung stehen. Bei der Weiterentwicklung des IT-Sicherheitsrechts muss daher ein besonderer Schwerpunkt auf die Sicherstellung der Vertrauenswürdigkeit von Technologie und digitalen Diensten gelegt werden, die auf dem internationalen Markt bezogen oder außerhalb Europas bereitgestellt werden.

2. Stand der Gesetzgebung zur IT-Sicherheit

Mit dem IT-Sicherheitsgesetz von 2015 hat Deutschland eine Vorreiterrolle bei der sektorübergreifenden Regulierung der IT-Sicherheit eingenommen und auch die EU-Richtlinie über Netzwerk- und Informationssicherheit (NIS-Richtlinie) von 2016 deutlich beeinflusst. Die Regelungen zur IT-Sicherheit kritischer Infrastrukturen haben ein hohes Niveau an IT-Sicherheit in den betroffenen Bereichen erreichen können. Das für die Umsetzung ganz wesentlich verantwortliche BSI wurde in seiner Leistungsfähigkeit gestärkt, hat zahlreiche neue Aufgaben übernommen und sich als Kompetenzträger in wichtige Digitalisierungsvorhaben eingebracht.

Die Regelungen des IT-Sicherheitsgesetzes haben sich insofern grundsätzlich bewährt. Angesichts der veränderten Gefährdungslage sind Weiterentwicklungen gleichwohl erforderlich. Die Produktsicherheit einschließlich der Vertrauenswürdigkeit von Produkten entlang der Lieferkette sind vom IT-Sicherheitsgesetz nicht adressiert. Weite Teile der deutschen Wirtschaft sind bislang nicht in ein gemeinsames Schutzkonzept und den Informationsaustausch eingebunden. Die Befugnisse des BSI gegenüber den Behörden des Bundes sind eingeschränkter als die Befugnisse gegenüber privaten Infrastrukturbetreibern. Gleichzeitig fehlen im deutschen Recht behördliche Befugnisse für eine aktive Cyberabwehr.

Diese Fragestellungen sollten bei einer Weiterentwicklung des IT-Sicherheitsrechts aufgegriffen werden. Gleichzeitig muss darauf geachtet werden, dass das IT-Sicherheitsrecht sich nicht zu einer Bremse für Innovation und Wettbewerbsfähigkeit der deutschen Wirtschaft entwickelt. Dies betrifft vor allem das Verhältnis des IT-Sicherheitsgesetzes zu weiteren IT-sicherheitsrechtlichen Vorschriften außerhalb dieses Gesetzes. Hier besteht schon heute eine Doppelregulierung, die zukünftig noch weiter ausgebaut werden wird.

Mit den Regelungen für Telemediendienste in § 13 Abs. 7 TMG (als Teil des IT-Sicherheitsgesetzes) und den Regelungen zur Datensicherheit in Art. 32 der Datenschutzgrundverordnung (DSGVO) sind seit 2015 IT-Sicherheitsanforderungen über KRITIS hinaus in weiteren Bereichen der Wirtschaft eingeführt worden. Sie

verpflichten viele Unternehmen, risikoangemessene und dem Stand der Technik entsprechende IT-Sicherheitsmaßnahmen zu ergreifen und Vorfälle zu melden. Kapitalgesellschaften sind überdies im Rahmen ihrer unternehmerischen Riusikovorsorge verpflichtet, grundlegende Vorkehrungen der IT-Sicherheit zu treffen. IT-Sicherheitsmaßnahmen sind zudem auf Grundlage deutscher und internationaler Prüfstandards Gegenstand der Abschlussprüfung bzw. gesonderter IT-Prüfungen.

Auch die sektorale Regulierung zur IT-Sicherheit hat in den letzten Jahren sprunghaft weiterentwickelt. Eine Fülle an Fachgesetzen der EU, des Bundes und der Länder stellt fachspezifische Anforderungen an die IT-Sicherheit, etwa in den Bereichen Banken und Versicherungen, Energie, Telekommunikation, Gesundheitswesen. Weitere Regelungen wie Cybersicherheits-Anforderungen an Fahrzeughersteller im Zulassungsrecht kommen derzeit hinzu.

Gleichzeitig hat die EU-Kommission am 16. Dezember 2020 einen Entwurf für eine Neufassung der NIS-Richtlinie vorgelegt. Er überschneidet sich erheblich mit den Regelungen des vorliegenden Entwurfes. Seine Verabschiedung wird dazu führen, dass das deutsche IT-Sicherheitsrecht erneut geändert werden muss. Das IT-Sicherheitsgesetz 2.0 sollte daher so gestaltet werden, dass es Vorbild für die europäische Regulierung sein kann und europäisch anschlussfähig ist.

Eine **Evaluierung** allein der Regelungen des IT-Sicherheitsgesetzes von 2015 würde diesem Zusammenspiel der Gesetze nicht ausreichend gerecht. Insbesondere für Wirtschaftsunternehmen besteht die Gefahr differierender IT-Sicherheits-anforderungen und Aufsichtsbefugnisse im IT-Sicherheits-, Datenschutz- und sektoralen Recht. Neben der Anpassung des BSI-Gesetzes durch den vorliegenden Entwurf ist daher eine umfassendere Betrachtung der IT-Sicherheitsregulierung erforderlich, die zu Beginn der 20. Wahlperiode des Deutschen Bundestags beauftragt werden sollte, um die Grundlage für nächste gesetzgeberische Schritte zu legen.

3. Stellungnahme zum Entwurf eines IT-Sicherheitsgesetzes 2.0

Der vorliegende Entwurf des IT-Sicherheitsgesetzes 2.0 entwickelt das IT-Sicherheitsrecht und das Instrumentarium des Staates zur Bewältigung der verschärften Cybersicherheitslage im Grundsatz sinnvoll weiter. Statt jahrelanger Beratung innerhalb der Bundesregierung hätte dem Entwurf allerdings eine breitere Erörterung mit Wirtschaft, Zivilgesellschaft und Wissenschaft gut getan. Denn der Entwurf ist sehr stark „vom Staat her gedacht“. Im Mittelpunkt der Überlegungen steht vor allem die Erweiterung von Aufgaben und Befugnisse des BSI.

Dies hat seine Berechtigung in Bereichen, in denen Vollzugsdefizite bestehen, etwa der **IT-Sicherheit in der Bundesverwaltung** oder der Einführung erster Maßnahmen

zur **technischen Gefahrenabwehr**. Maßnahmen zur technischen Gefahrenabwehr im Cyberraum sind bislang nur schwach ausgeprägt. Zwar haben Telekommunikationsanbieter im Jahr 2017 zusätzliche Möglichkeiten für ihren Bereich erhalten, das BSI hat ihnen gegenüber jedoch nur eine empfehlende Rolle und kann keine Maßnahmen anordnen. Zudem fehlt in Deutschland eine Rechtsgrundlage für aktive Cyberabwehrmaßnahmen, die sich gegen Täter im In- und Ausland richten. Hier sind die im Gesetzentwurf vorgeschlagenen Befugniserweiterungen geeignet, das BSI-Instrumentarium zu erweitern, lageangemessen zu reagieren.

Zu bedenken ist hierbei, dass mit den neuen Befugnissen eine Erweiterung der Verantwortungsübernahme durch das BSI verbunden ist. Aus der Aufgabenstellung und den damit verbundenen neuen Befugnissen entsteht jeweils auch eine Verpflichtung des BSI, eine Notwendigkeit zum Nutzen dieser Gefahrenabwehrbefugnisse zu prüfen. Jede beim BSI eingehende Information über bestimmte technische Sachverhalte kann in geeigneter Kombination mit vorhandenen BSI-Erkenntnissen zu der Gesamtbewertung einer bevorstehenden Gefahr für Bürgerinnen und Bürger, Unternehmen oder Behörden führen. Erkennt das Amt diese Gefahrenlage nicht oder macht von seinen Gefahrenabwehrbefugnissen nicht, unzureichend oder zu spät Gebrauch, werden die Betroffenen das BSI für die unterlassenen Maßnahmen verantwortlich machen.

Wenig überzeugend ist der Gedanke der Herstellung von IT-Sicherheit durch Aufgaben- und Befugniserweiterung des BSI bei dem **Schutz der deutschen Wirtschaft**. Der Zusammenarbeit von Staat und Wirtschaft bei der Cybersicherheit kommt eine überragende Bedeutung zu. Einer netzwerkförmigen Bedrohungs wie im Cyberraum kann nicht durch eine sternförmige, zentralistische Abwehrstrategie begegnet werden. Zwar existieren eine Reihe von gemeinsamen Aktivitäten, Vereinen und Kooperationen von Staat und Wirtschaft. Sie sind jedoch bislang nicht mit dem regulatorischen Konzept des IT-Sicherheitsgesetzes verknüpft. Das Gesetz schafft keine institutionalisierte Einbindung der Wirtschaft in ein gemeinsames Schutzkonzept, die sich an alle Unternehmen in Deutschland richtet.

Die IT- und Cybersicherheit der Unternehmen in Deutschland kann verbessert werden, wenn die Unternehmen dazu angehalten werden, selbst entsprechende Maßnahmen innerhalb des Unternehmens zu ergreifen und vertrauensvoll miteinander und mit den Behörden zusammenzuarbeiten. Unternehmen müssen ein umfassendes und risikoangemessenes IT-Sicherheitsmanagement aufbauen, das von Geschäftsführung und Aufsichtsgremien regelmäßig geprüft. Dies kann nicht durch Berichtspflichten, Prüfungen und Hinweise des BSI ersetzt werden. Die Komplexität der IT-Infrastrukturen und ihre Vernetzung erfordern stets eine aufwändige Analyse, um die IT-Sicherheit eines Unternehmens belastbar beurteilen zu können. Zudem muss sich die IT-Infrastruktur und -Anwendungslandschaft der Unternehmen im Hinblick auf den Erhalt der Wettbewerbsfähigkeit beständig verändern. Angemessene IT-Sicherheit

muss daher in die unternehmenseigenen Prozesse integriert werden und kann nicht im Einzelfall von außen durch den Staat definiert und kontrolliert werden. Eine zu kleinteilige staatliche Regulierung hat einen gleich doppelt negativen Effekt: Erstens wird das Unternehmen wird aus der Verantwortung genommen, selbst nach adäquaten Sicherheitsmaßnahmen zu suchen. Zweitens wird Innovation im Unternehmen und damit auch die Wettbewerbsfähigkeit behindert, wenn staatlich „abgenommene“ Informationstechnik nicht geänderten Anforderungen angepasst werden kann.

Eine ganzheitliches Schutzkonzept für die Wirtschaft über KRITIS hinaus muss insofern auf Rahmenvorgaben für das Risikomanagement der Unternehmen, auf die Selbstregulierung innerhalb der Branchen, auf die Förderung eines engen Informationsaustausch zwischen den Unternehmen, auf staatliche Hilfsangebote sowie auf die Kooperation zwischen Staat und Wirtschaft setzen. Diesem Ansatz werden die Regelungen in dem Gesetzentwurf nicht ausreichend gerecht.

Weitere Bereiche der Wirtschaft sollen durch den Entwurf in die Regulierung einbezogen werden, ohne dass der Kreis der Betroffenen, die Schutzziele und die zu ergreifenden Maßnahmen klar definiert sind. Das Schutzkonzept beschränkt sich im Wesentlichen auf eine Verpflichtung von Unternehmen zur Weiterleitung von Unterlagen an das BSI und zur Meldung von Vorfällen. Der Entwurf überlässt es weitgehend dem Ermessen des BSI, ob und welche Maßnahmen ergriffen werden und welcher Mehrwert sich für den Schutz des Unternehmens aus der Informationszulieferung ergibt. Es gibt (außerhalb von KRITIS) keine Verpflichtung für das BSI, die Unternehmen in bestimmten Gefahrensituationen zu informieren. Weder werden konkrete Hilfestellungen der Behörden, wie etwa die Sicherheitsüberprüfung von IT-Administratoren, geregelt noch ein System des wechselseitigen Informationsaustausches vorgesehen, wie es beispielsweise Art. 26 des Entwurfs der NIS-Richtlinie 2 vorschlägt. Auch eine Incentivierung von Selbstregulierung innerhalb der Branchen, der für kritische Infrastrukturen in § 8a Abs. 2 BSIG vorgesehen ist, wird durch den Entwurf nicht auf andere Teile der Wirtschaft übertragen.

Zu begrüßen ist, dass der Entwurf erstmals in größerem Umfang die Frage der **Produktsicherheit** und der Vertrauenswürdigkeit von Komponenten entlang der Lieferkette adressiert. Der erfolgreiche Angriff auf Unternehmen und Behörden über die Netzwerksoftware von SolarWinds zeigt deutlich die Bedeutung, die der Sicherheit von eingekauften Komponenten oder Diensten von Drittanbietern zukommt. Mit dem IT-Sicherheitskennzeichen wird ein grundsätzlich geeignetes Instrument zur Verbesserung der IT-Sicherheit für Verbraucher eingeführt. Das Kennzeichen sollte jedoch als Übergangslösung verstanden werden, weil es hier einer einheitlichen Lösung für den europäischen Binnenmarkt bedarf, die auf Basis der europäischen Cybersicherheitszertifizierung gefunden werden muss. Bedauerlich ist, dass das IT-Sicherheitskennzeichnen nach der Entwurfsfassung ausdrücklich keine Aussage im

Hinblick auf den Datenschutz der Produkte trifft. Im Hinblick auf die Verpflichtungen zur IT-Sicherheit aus Art. 32 DSGVO wären solche Aussagen für die Marktteilnehmer gerade hilfreich gewesen.

Die Regelungen zur Sicherheit kritischer Kernkomponenten sind ein Einstieg in eine allgemeine Regulierung kritischer IT-Produkte. Der im Gesetzentwurf derzeit auf die Telekommunikation eingeschränkte Anwendungsbereich kann leicht durch sektorales Recht erweitert werden. Auch die EU-Kommission verfolgt mit Art. 21, 22 des Entwurfs der NIS-Richtlinie 2 ähnliche Ansätze. Die Erfordernis einer Cybersicherheits-zertifizierung kritischer Komponenten ist zu begrüßen. Das Zertifizierungsverfahren muss allerdings so ausgestaltet werden, dass sich aus einer Ausweitung von Zertifizierungspflichten keine universelle Innovationsbremse für weite Bereiche der Informationstechnik ergeben. Die Möglichkeit der Hersteller zur schnellen Weiterentwicklung von Technologie ist auch im Interesse der IT-Sicherheit sinnvoll.

Die Verknüpfung der technischen Prüfung mit einer komponentenbezogenen politisch motivierten „Vertrauenswürdigkeitsprüfung“ überzeugt allerdings nicht. Angesichts der globalen Cybersicherheitslage und der gegen die Sicherheitsinteressen Deutschlands und Europas gerichteten Cyberstrategien Russlands und Chinas ist die sicherheits-politische Bewertung der Digitalisierung gerade im Bereich der kritischen Infrastrukturen von höchster Bedeutung. Eine solche sicherheitspolitische Entscheidung kann nicht in einem bürokratisierten Verfahren entlang des Einsatzes einzelner Komponenten erfolgen. Dies ist für die Betreiber der Infrastrukturen unpraktikabel, weil keine Verlässlichkeit über die Möglichkeit des Einsatzes der Produkte eines Herstellers besteht. Gleichzeitig erschwert ein solches, umfassend gerichtlich überprüfbares Verwaltungsverfahren auch die notwendigen sicherheits-politischen Abstimmungen mit den Partnern in der EU und der NATO. Zudem beschneidet das bürokratische Verfahren des Entwurfs die Möglichkeiten der Bundesregierung, mit Herstellerländern in politische Verhandlungen einzutreten.

4. Stellungnahme zu einzelnen Regelungen

(a) Schutz der Bundesverwaltung

Die Regelungen zur Verbesserung des Schutzes der Bundesverwaltung und der Kommunikationstechnik des Bundes (§§ 4, 4a, 5a, 8 BSIG-E) sind im Großen und Ganzen geeignet, die bestehenden Defizite zu verringern.

1. Nicht nachvollziehbar sind die **Ausnahmen für Teile der Bundesverwaltung**. Ausgerechnet für sensible Bereiche der Bundesverwaltung wie das Auswärtige Amt oder die Bundeswehr sollen die neuen Regelungen nur eingeschränkt gelten (§ 2 Abs. 3 Satz 2 BSIG-E). Vollkommen unverständlich ist die Tatsache, dass

neben dem Bundestag auch Bundesrat, Bundesverfassungsgericht und sogar der Bundesrechnungshof aus der Geltung des BSI-Gesetzes weitgehend herausgenommen sind. Wie Brandschutz- oder Arbeitsschutzregelungen ganz selbstverständlich auch für diese Einrichtungen gelten, sollten sie bei der IT-Sicherheit nicht schwächer geschützt sein als die übrigen Einrichtungen des Bundes. Hier wird empfohlen, die Ausnahmeklauseln sehr viel enger zu fassen, etwa allein den militärischen Bereich der Bundeswehr auszunehmen.

2. Während das BSI für die von dem IT-Sicherheitsgesetz betroffenen Branchen vielfältige **Mindestanforderungen** allein nach Anhörung der Branchenverbände erlassen kann, sind entsprechende Befugnisse des BSI für den Bereich des Bundes eingeschränkt. Nach § 8 Abs. 1 Satz 1 BSIG-E erfordert der Erlass von Mindeststandards durch das BSI ein Einvernehmen mit allen Ressorts. Die IT-Sicherheitsanforderungen für den Bund sollten nicht durch einzelne Ministerien blockiert werden können. Hier sollte zu einer früheren Entwurfsfassung zurückgekehrt werden.

- Artikel 1 Nummer 11a: In Absatz 1 sollte „Einvernehmen“ durch „Benehmen“ ersetzt werden.

(b) Schutz der deutschen Wirtschaft

1. Die vom Entwurf vorgesehene Einbeziehung weitere Bereiche der deutschen Wirtschaft in die IT-Sicherheitsregulierung ist grundsätzlich zu begrüßen. Nicht überzeugend ist das Konzept der Einbeziehung von Unternehmen, die nach ihrer inländischen Wertschöpfung zu den **größten Unternehmen Deutschlands** gehören (§ 2 Abs. 14 Satz 1 Nummer 2 BSIG-E). Die Einbeziehung in die Regulierung muss hinsichtlich des Adressatenkreises, des Schutzgegenstandes und des Schutzziels für die Normunterworfenen transparent sein. Dies ist im gegenwärtigen Entwurf nicht der Fall.

   Bei Betreibern kritischer Infrastrukturen wird der Anwendungsbereich über die Definition bestimmter kritischer Dienstleistungen eines Unternehmens und der dafür benötigten IT-Systeme eingeschränkt und damit handhabbar gemacht. Für die nach inländischer Wertschöpfung größten Unternehmen erfolgt jedoch keine hinreichende gesetzliche Bestimmung der Adressaten und des zu schützenden Bereichs. Auch wird in keiner Weise einschränkend definiert, mit welchem Schutzziel sie ihre IT zu schützen haben. Stattdessen sollen die Unternehmen eine umfassende Selbsterklärung über ihre gesamte IT abgeben, zu der dann das BSI „Hinweise“ (§ 8f Abs. 3 BSIG-E) geben soll. Ein solches Vorgehen überfordert beide Seiten, das Unternehmen ebenso wie das BSI, ohne dass damit ein belastbarer Gewinn an IT-Sicherheit verbunden wäre.

Die EU-Kommission verfolgt mit dem Entwurf der NIS-Richtlinie 2 ein anderes, transparenteres Konzept. Dort wird der Kreis der zu regulierenden Unternehmen in Anlehnung an die kritischen Infrastrukturen branchenspezifisch weiterentwickelt. Dieses branchenweise Vorgehen hat den Vorteil, das nachvollziehbare Schwellwerte definiert und auch eine Kohärenz mit den IT-Sicherheitsregelungen in den branchenspezifischen Fachgesetzen hergestellt werden kann. Die Erweiterung des Kreises der Unternehmen sollte daher bis nach Verabschiedung der NIS-Richtlinie 2 zurückgestellt werden. Parallel zur Beratung der Richtlinie könnten BMI und Wirtschaftsverbände weitere Konkretisierungen ausarbeiten.

- Artikel 1 Nr. 1e (§ 2 Abs. 14 Satz 1 Nummer 2 BSIG-E)
  Die Gruppe der Unternehmen, die nach inländischer Wertschöpfung zu den größten Unternehmen Deutschlands gehören, sollte aus dem Anwendungsbereich gestrichen werden (mit Folgeänderungen).

Ersatzweise könnte der deutsche Gesetzgeber wie auch mit dem ersten IT-Sicherheitsgesetz eine Vorlage für eine geeignete branchenspezifische Erweiterung der IT-Sicherheitsregulierung schaffen, die dann auch in die Verhandlungen auf EU-Ebene eingebracht wird.

- In Artikel 1 Nr. 1e (§ 2 Abs. 14 Satz 1 Nummer 2 BSIG-E) könnte analog zu § 2 Abs. 10 BSIG eine Liste von Branchen aufgeführt werden.
- Artikel 1 Nummer 20b (§ 10 Abs. 6 BSIG-E): Die Verordnungsermächtigung ist entsprechend zu ändern, um Branchenleistungen und Schwellwerte festzulegen.

2. Von zentraler Bedeutung für die Gewährleistung von IT-Sicherheit in den Unternehmen ist die **personelle Sicherheit**. Insbesondere die für die IT-Administration verantwortlichen Mitarbeiterinnen und Mitarbeiter müssen hohe Anforderungen an die Vertrauenswürdigkeit erfüllen. In Vorentwürfen des Gesetzentwurfs war daher die Möglichkeit einer Sicherheitsüberprüfung des entsprechenden Personals (Ü1) vorgesehen. Dies sollte wieder aufgenommen werden.

- In Artikel 1 Nummer 12 (§ 8a Abs. 1 BSIG-E) sollte eine den Vorentwürfen entsprechende Regelung wieder aufgenommen werden.
- In Artikel 1 Nummer 17 (§ 8f BSIG-E) sollte eine entsprechende Anwendung für Unternehmen im besonderen öffentlichen Interesse vorgesehen werden.

3. Für kritische Infrastrukturen sieht das geltende Recht eine Incentivierung branchenspezifischer Selbstregulierung vor, indem die Möglichkeit eingeräumt wird, **branchenspezifische Sicherheitsstandards** (B3S) zu erarbeiten und vom BSI anerkennen zu lassen (§ 8a Abs. 2 BSIG). Hiervon wurde vielfältig Gebrauch gemacht. 12 B3S sind vom BSI anerkannt, weitere zwei im Verfahren. Diese Möglichkeit sollte auch bei Unternehmen im besonderen öffentlichen Interesse vorgesehen werden.

- In Artikel 1 Nummer 17 (§ 8f BSIG-E) sollte an geeigneter Stelle ein § 8a Abs. 2 BSIG entsprechendes Verfahren vorgesehen werden.

4. Eine **Bereitstellung von Informationen durch das BSI für die Unternehmen** ist nur im KRITIS-Bereich verpflichtend vorgesehen. Der Schutz der deutschen Wirtschaft vor Cyberangriffen erfordert es, dass das BSI auch über den KRITIS-Bereich hinaus Informationen weitergibt, die für die Sicherheit der Unternehmen bedeutend sind. Das BSI sollte entsprechend verpflichtet werden.

- In Artikel 1 Nummer 3 (§ 4b Abs. 3 BSIG-E) sollte die Formulierung „soll die gemäß Absatz 2 gemeldeten Informationen nutzen“ durch „nutzt die gemäß Absatz 2 gemeldeten Informationen“ ersetzt werden.

(c) Kritische Kernkomponenten

Die Definition kritischer Kernkomponenten und die Einführung eines Verfahrens zur stärkeren Kontrolle ihrer Sicherheit und der Vertrauenswürdigkeit ist zu begrüßen. Das in § 9b BSIG-E vorgesehene Verfahren vermischt jedoch die technische Prüfung von Komponenten und die sicherheitspolitische Bewertung der Vertrauenswürdigkeit von Herstellern in ungünstiger Art und Weise. Dass kritische Kernkomponenten einer IT-Sicherheitszertifizierung bedürfen, sofern dies gesetzlich angeordnet wird, ist zu unterstützen.

Das zusätzliche Erfordernis der Garantieerklärung des Herstellers stellt aber über die im Rahmen der Zertifizierung geprüften technischen Anforderungen hinaus keine nennenswerten weiteren Anforderungen auf, die helfen könnten, die sicherheitspolitische Frage der Vertrauenswürdigkeit des Herstellers zu überprüfen. Sowohl die gesetzlichen Anforderungen an die Inhalte der Garantieerklärung (§ 9b Abs. 2 Satz 4 BSIG-E) wie auch an die Vertrauenswürdigkeit eines Herstellers (§ 9b Abs. 5 BSIG-E) beziehen sich allein auf die technische Leistungsfähigkeit und Qualität.

Sicherheitspolitische Fragen der Vertrauenswürdigkeit wie die Abhängigkeit des Herstellers von ausländischen Regierungen, die Beteiligungsstruktur, die Mitwirkung an nachrichtendienstlichen Operationen, die Besetzung von Führungsfunktionen

durch regierungsnahes Personal, die Kontrollmöglichkeiten deutscher Behörden im Hinblick auf die für Sicherheitsfragen zuständigen Unternehmensteile etc. sind nicht Gegenstand der Definitionen.

Solche Fragestellungen sollen allein in dem 30-Tage-Zeitraum nach Anzeige des Einsatzes einer Komponente (§ 9b Abs. 3 BSIG-E) geprüft werden. Diese Frist ist zu kurz. Eine substantiierte Prüfung und anschließende ministerielle und politische Abstimmung innerhalb der Bundesregierung wird in der Regel nicht möglich sein. Sollten in dem Zeitraum keine ausreichenden Erkenntnisse vorliegen, ist anschließend eine sicherheitspolitische Bewertung nicht mehr ohne weiteres möglich. Lediglich der Verlust der – dann aber nur auf technische Faktoren bezogenen – Vertrauenswürdigkeit kann (nach § 9b Abs. 4 BSIG-E) zu einem späteren Ausschluss dieser Komponente oder (nach Abs. 6, 7) weiterer Komponenten des Herstellers führen.

Allein komponentenbezogene Prüfungen schränken die sicherheitspolitischen Handlungsmöglichkeiten der Bundesregierung, auch im Zusammenwirken in der EU und der NATO, erheblich ein. Eine gemeinsame sicherheitspolitische Bewertung, dass ein Hersteller beispielsweise mit ausländischen Nachrichtendiensten verquickt ist, lässt sich in dem bürokratischen Verfahren der komponentenbezogenen Vertrauenswürdigkeitsprüfung nicht adäquat berücksichtigen. Auch wäre kein politischer Spielraum gegeben, in bilateralen Verhandlungen mit Herstellerstaaten Übereinkünfte zu gegenseitigen vertrauensbildenden Maßnahmen im Hinblick auf Komponentenhersteller kritischer Infrastrukturen einschließlich einer Reziprozität zu vereinbaren.

Daher sollte die technische Zertifizierung von Komponenten entkoppelt werden von einer sicherheitspolitischen Prüfung der Vertrauenswürdigkeit der Hersteller. Letzteres könnte losgelöst von einzelnen Komponenten durch eine **sicherheitspolitische Unbedenklichkeitsbescheinigung hinsichtlich des Herstellers** durch das BMI gegenüber dem Betreiber der kritischen Infrastruktur abgebildet werden.

- Artikel 1 Nummer 19 (§ 19 b Abs. 2 BSIG-E) sollte so formuliert werden, dass Voraussetzung für den Einsatz einer Komponente eine von der Bundesregierung festgestellte Unbedenklichkeitsbescheinigung hinsichtlich des Herstellers ist.
- Artikel 1 Nummer 19 (§ 19 b Abs. 3 BSIG-E) sollte die Grundsätze und das Verfahren der Unbedenklichkeitsbescheinigung festlegen. Die Bescheinigung sollte Ergebnis einer Prüfung der sicherheitspolitischen Zuverlässigkeit sein und vom BMI nach Konsultation des Bundessicherheitsrates für einen Zeitraum von 3-5 Jahren erteilt werden.
- Artikel 1 Nummer 19 (§ 19b Abs. 4 BSIG-E) sollte die Voraussetzungen, das Verfahren und die Rechtsfolgen des Entzugs der Unbedenklichkeitsbescheinigung beschreiben. Ein Entzug sollte nur in

Betracht gezogen werden, wenn schwerwiegende Hinweise auf eine sicherheitspolitische Unzuverlässigkeit vorliegen.
- Artikel 1 Nummer 19 (§ 19b Abs. 5 BSIG-E) sollte Übergangsregelungen für im Einsatz befindliche Komponenten formulieren.
- Artikel 1 Nummer 19 (§ 19b Abs. 6 BSIG-E) sollte entfallen.

(d) Technische Vorgaben durch den Staat und Offenlegungspflichten

Der Entwurf schafft neue rechtliche Möglichkeiten für das BSI und die Bundesregierung, IT-Produkte für den deutschen Markt zu standardisieren. Solche staatlichen Vorgaben für konkrete Produkte müssen eine Ausnahme sein, weil sie Produktinnovation erschweren, eine am Markt stattfindende Standardisierung behindern und den deutschen Markt international entkoppeln. Gerade bei Sicherheitstechnologien, die für zahlreiche deutsche Branchen integraler Bestandteil ihrer Produkte sind, hängen die Innovations- und Wettbewerbsfähigkeit der Unternehmen von schneller Innovation ab, die nicht durch Rechtsverordnungen oder Verwaltungsvorschriften erfolgen sollte. Staatliche Vorgaben behindern zudem international agierende Unternehmen mit weltweiten Produktionsstätten bei der Vereinheitlichung und Konsolidierung ihrer IT-Infrastrukturen.

1. Die in § 2 Nr. 20 BSIG-E neu vorgesehene Möglichkeit für das BSI, den Stand der Technik bei der IT-Sicherheit festzulegen, beendet das bewährte und auf der Rechtsprechung des Bundesverfassungsgerichts beruhende Konzept einer dynamischen Verweisung. Der Normadressat, zum Beispiel ein Unternehmen, soll nach der bisherigen Verwendung des Begriffs „Stand der Technik“ verpflichtet sein, die gesetzlichen Schutzziele unter Zugrundelegung der zum jeweiligen Zeitpunkt geeigneten technischen Mittel zu erreichen. Dies hat einen Vorteil für das Unternehmen, das aus mehreren Mitteln auswählen kann, und einen Vorteil für die Allgemeinheit, weil der Normadressat die technischen Mittel – beispielsweise bei veränderter Gefährdungslage – selbständig anpassen muss.

   Eine **Definition des „Standes der Technik“** durch das BSI würde beide Vorteile zerstören. Sicherheitsinnovation würde verhindert, das BSI durch eine Pflicht zur permanenten Aktualisierung von Dokumenten restlos überfordert werden.

- In Artikel 1 Nummer 2g (§ 3 Abs. 1 Satz 2 BSIG-E) sollte Nr. 20 gestrichen werden.

2. Eine neue **Verordnungsermächtigung in § 10 Abs. 6 BSIG-E** soll dem BMI die Möglichkeit geben, für alle informationstechnischen Systeme Interoperabilität und Standards festzulegen. Zudem soll zu Zwecken der IT-Sicherheit, aber auch zu dem Zweck der „Kontrolle“ eine Offenlegung beliebiger informationstechnischer Schnittstellen angeordnet werden können.

   Eine solche Verordnungsermächtigung erlaubt tiefgreifende und in der Allgemeinheit der Formulierung nicht mehr zu rechtfertigende Eingriffe des Staates in alle IT-Systeme in Deutschland. Nach dem Wortlaut des Entwurf gilt sie für jedes informationstechnische System, mithin für die Notebooks und Smartphones der Bürgerinnen und Bürger ebenso wie für die IT-Systeme in Banken und Chemieanlagen. Abgesehen von den verfassungs- und europarechtlichen Bedenken gegen eine so umfassende Ermächtigung zur Regulierung von Unternehmen und Märkten behindern solche Vorgaben zur Ausgestaltung von Technik einschließlich einzusetzenden Sicherheitstechnologien und -maßnahmen jegliche Produktinnovation und angesichts der Bedeutung der IKT damit die Innovationsfähigkeit der Wirtschaft insgesamt.

   Die Zweckbestimmung der Verordnungsermächtigung ist so allgemein, dass der Verordnungsgeber daneben eine Offenlegung jeder beliebigen Schnittstelle jedes beliebigen deutschen IT-Systems verlangen könnte. Eine solche staatliche Anordnung der Offenlegung von Schnittstellen führt nicht zu mehr Sicherheit, sondern kann zu erheblichen Risiken für die Unternehmen führen. Nicht nur ist der Schutz getätigter Investitionen gefährdet, auch die Sicherheitsmaßnahmen von Unternehmen, etwa kryptografische Verfahren, könnten einer solchen Offenlegungsverpflichtung unterfallen.

   Der Wirtschaftsstandort Deutschland würde durch diese Verordnungsermächtigung einen erheblichen Nachteil erfahren, zumal die Regulierung ausschließlich für Deutschland gelten würde. Sie führt nicht nur zu einem Wettbewerbsnachteil, es behindert bei international agierenden Unternehmen mit weltweiten Produktionsstätten sowie weltweit vernetzten Zulieferströmen auch die Vereinheitlichung und Harmonisierung von IT-Infrastrukturen.

   - In Artikel 1 Nummer 20b wird der neue § 10 Abs. 6 BSIG-E gestrichen.

   Soll die Verordnungsermächtigung sich, wie die Begründung nahelegt, ausschließlich auf Interoperabilitätsanforderungen im Zusammenhang mit der OpenRAN-Technologie beziehen, könnte sie textlich eingeschränkt werden, indem „informationstechnische Systeme“ durch „Telekommunikationsnetze“ ersetzt werden. Eine solche Ermächtigung wäre sinnvoll (auch wenn das TKG hierfür der bessere Standort wäre).

5. Offene Fragen für die nächste Wahlperiode

Mit der Verabschiedung des vorliegenden Entwurfs wird das IT-Sicherheitsrecht bei Übernahme der Vorschläge in Abschnitt 4 sinnvoll weiterentwickelt. Durch das Ende der Wahlperiode ist es nicht möglich, weitere, langfristig notwendige Themen gesetzgeberisch aufzugreifen.

Für die kommende Wahlperiode des Deutschen Bundestages sehe ich folgende Schwerpunkte, die im gegenwärtigen Gesetzgebungsverfahren aus Zeitgründen nicht mehr möglich sind:

(a) Aktive Cyberabwehr

Der Entwurf entwickelt die Instrumente des Bundes für eine aktive Cyberabwehr mit den Untersuchungs-, Detektions- und Anordnungsbefugnissen des BSI sinnvoll weiter. Alle Befugnisse richten sich allein gegen Täter im Inland und an sonstige Verpflichtete im Inland, die bei der Abwehr unterstützen. Keine Befugnisse für die Behörden des Bundes enthält der Entwurf für Fälle, in denen ein Cyberangriff aus dem Ausland erfolgt und sich eine technische Abwehrmaßnahme unmittelbar gegen einen Server im Ausland richten müsste, um eine gegenwärtige Gefahr abzuwehren. Hier sollte – im Idealfall in enger Abstimmung mit europäischen Partnern – eine ergänzende Befugnis geschaffen werden.

(b) Cybersicherheitsarchitektur

Der Entwurf entwickelt vor allem die Regulierungs- und Cyberabwehrbefugnisse des BSI weiter und bewegt sich dabei im Hinblick auf die Gesetzgebungszuständigkeit des Bundes auf einer eher dünnen verfassungsrechtlichen Grundlage. Offen bleibt, wie sich Gefahrenabwehrbefugnisse des Bundesamtes zu den grundsätzlich den Ländern zustehenden polizeilichen Gefahrenabwehrbefugnissen verhalten. Zunächst sind die vom Bundesrat geforderten Unterrichtungen von Landesbehörden sinnvoll, um das Risiko unterschiedliches Vorgehens zu verringern. Langfristig ist aber einerseits eine institutionelle Anbindung der Länder an die Strukturen des Bundes, vor allem das Cyber-Abwehrzentrum, erforderlich, sowie andererseits eine präzisere Definition der Reichweite der Gefahrenabwehrkompetenz des Bundes im Cyberraum, etwa in Form einer Änderung des Grundgesetzes.

(c) Umgang mit Schwachstellen

Mit der Weiterentwicklung von Aufgaben und Befugnissen des BSI und der parallel dazu, in anderen Gesetzgebungsverfahren erfolgenden Weiterentwicklung der Befugnisse anderer Sicherheitsbehörden zur Online-Durchsuchung und Quellen-TKÜ

stellt sich zunehmend die Frage eines Umgangs der Bundesbehörden mit Schwachstellen in Hardware und Software. Einerseits strebt das BSI entsprechend seines gesetzlichen Auftrags, diese Schwachstellen jeweils schnellstmöglich zu schließen. Andererseits haben andere Sicherheitsbehörden des Bundes und der Länder das Interesse, bestimmte für die technische Umsetzung von Online-Durchsuchung und Quellen-TKÜ genutzte Schwachstellen weiter zu nutzen. Der vorliegende Gesetzentwurf stellt in begrüßenswerter Weise in den §§ 7a, 7b BSIG-E klar, dass die Aufgabenerfüllung des BSI keine ausdrückliche Rücksicht auf die Interessen anderer Sicherheitsbehörden nehmen soll. Diese ersten Ansätze einer Regelung des Komplexes kann aber eine umfassende Regelung eines institutionalisierten Abwägungsprozesses (Vulnerability Equities Process) nicht ersetzen.

(d) Von der Mehrfachregulierung zum IT-Sicherheitsrecht AT

Das IT-Sicherheitsrecht hat sich seit dem IT-Sicherheitsgesetz von 2015 stürmisch weiterentwickelt. Mehr als 70 Gesetze und Verordnungen des Bundes regeln sektorspezifische Anforderungen. Mit dem IT-Sicherheitsgesetz 2.0 und der NIS-Richtlinie 2 wird auch das allgemeine IT-Sicherheitsrecht weiterentwickelt. Gleichzeitig beziehen andere Rechtsquellen, etwa das Haftungsrecht oder die Grundsätze ordnungsgemäßen Unternehmensführung, zunehmend IT-Sicherheitsanforderungen ein. Dies ist grundsätzlich sachgerecht. Ähnlich wie das und parallel zu dem Datenschutzrecht greift das IT-Sicherheitsrecht in alle Lebensbereiche ein. Anders als beim Datenschutz fehlt aber bislang eine Struktur des Rechtsgebiets, die grundlegende Definitionen, Grundsätze der Vorsorge und Verantwortungsverteilung, der Aufsicht und des Zusammenwirkens „vor die Klammer“ zieht. Um eine inkonsistente Mehrfachregulierung zu vermeiden, sollte in der nächste Wahlperiode die Grundlage gelegt werden, einen allgemeinen Teil des IT-Sicherheitsrechts zu schaffen, der dem neuen Rechtsgebiet auf europäischer und nationaler Ebene eine Ordnung gibt und die Weiterentwicklung erleichtert.

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
19(4)741 E

Rheinische Friedrich-Wilhelms-Universität Bonn
Rechts- und Staatswissenschaftliche Fakultät

An den Ausschuss für Inneres und Heimat
des Deutschen Bundestags
z. Hd. der Vorsitzenden

Prof. Dr. Klaus F. Gärditz
Institut für Öffentliches Recht
Postanschrift:
Adenauerallee 24-42
53113 Bonn
Tel.: 0228/73-9176
Email: gaerditz@jura.uni-bonn.de

Bonn, den 28. Februar 2021

Stellungnahme zum Entwurf eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme

Der Regierungsentwurf des Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (BT-Drs. 19/26106) zielt auf eine Fortentwicklung des 2015 geschaffenen IT-Sicherheitsgesetzes.[1] Das Gesetz trägt insgesamt den gewachsenen Gefährdungen digitaler Infrastrukturen Rechnung und versucht, die digitale Infrastrukturgewährleistungsverantwortung des Bundes und das BSI als insoweit operativ zuständige Behörde zu stärken. Die neuen §§ 4a, 4b, 7a-7d, 9a BSIG-E zentralisieren im Einklang mit Art. 87 Abs. 3 Satz 1 GG Zuständigkeiten und Verantwortung beim BSI, dessen Charakter als technik- und infrastrukturbezogene Sicherheitsbehörde insoweit ausgeschärft wird. Dies ist grundsätzlich zu begrüßen, zumal die hier thematischen Gefährdungen in besonderem Maße komplexes Fachwissen erfordern, das sinnvollerweise zentral generiert, gebündelt und operationalisiert werden muss. Die hierbei eingeschlossene Regelung des § 5c BSIG-E über die Bestandsdatenauskunft genügt namentlich den jüngsten[2] Anforderungen des BVerfG.[3]

Da ich mich nur als wissenschaftlicher Sachverständiger für Verfassungs- und Sicherheitsrecht, nicht aber für Technik- und Informationsrecht aus eigener Fachkompetenz äußern kann, möchte ich meine Stellungnahme auf eine Regelung konzentrieren, die im Zusammenhang mit dem 5G-Ausbau steht und politisch besonders sensibel ist: die Untersagung des Einsatzes kritischer Komponenten nach § 9b BSIG-E. Diese Regelung reagiert auf die kontroversen Diskussionen auch in anderen Ländern, inwiefern es mit der „digitalen Souveränität“ und dem Bedarf an Sicherheit sowie Vertraulichkeit der auszubauenden TK-

[1] Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme v. 17.7.2015 (BGBl. I 2015 S. 1324).

[2] BVerfG, Beschl. v. 27.5.2020 – 1 BvR 1873/13, CR 2020, 607 (Bestandsdatenauskunft II).

[3] Vgl. auch BVerfGE 154, 152 Rn. 148 ff.; BT-Drs. 19/26106, S. 64.

Netze vereinbar ist, „Kritische Komponenten“ (§ 2 Abs. 13 BSIG-E) von Anbietern einzusetzen, die unter dem Einfluss fremder Staaten stehen, die Sicherheitslücken ausnutzen bzw. technische Infrastruktur-Mitbeherrschung (etwa zu Spionage oder Sicherheitsgefährdung) missbrauchen könnten. Dies ist zwar nach dem Regelungsziel sachgerecht und für einen demokratischen Rechtsstaat zwingend notwendig. Das gilt namentlich für den Ausschluss von Komponenten, die über technische Eigenschaften verfügen, „die geeignet sind, missbräuchlich, insbesondere zum Zwecke von Sabotage, Spionage oder Terrorismus auf die Sicherheit, Integrität, Verfügbarkeit oder Funktionsfähigkeit der Kritischen Infrastruktur einwirken zu können“ (§ 9b Abs. 2 Satz 4 BSIG-E). Jedoch erweist sich der konkrete Regelungsinhalt sowohl als verfassungsrechtlich angreifbar als auch als dysfunktional. Die Regelung des § 9b BSIG-E ist kein Beitrag, sicherheitsrechtliche Befugnisse des Bundes zu stärken; die verfassungswidrig unbestimmte Regelung ist vielmehr darauf ausgerichtet, die Wahrung der inneren und äußeren Sicherheit in Bezug auf den TK-Netzausbau weitgehend dem politischen Ermessen der Regierung zu überlassen, insoweit aber eine Intervention bei der Verwendung bedenklicher Komponenten weitestgehend zu erschweren.

Hierzu darf ich im Einzelnen wie folgt Stellung nehmen:

I. Vorbehalt des Gesetzes

Verfassungsrechtliche Zweifel an der Regelung des § 9b BSIG-E ergeben sich vor allem im Hinblick auf den demokratischen und grundrechtlichen Vorbehalt des Gesetzes.

Der Vorbehalt des Gesetzes beruht auf der Prämisse, dass Gemeinwohl im demokratischen Rechtsstaat fortwährend erst durch politische Entscheidungen in normsetzenden Verfahren hergestellt werden muss.[4] Der rechtsstaatliche Vorbehalt des Gesetzes (verwurzelt in Art. 20 Abs. 3 GG[5]) soll die Berechenbarkeit, Normgeleitetheit und Kontrollierbarkeit der Rechtsanwendung sicherstellen. Er sichert die Berechenbarkeit sowie Kontrollierbarkeit der Rechtsanwendung und wirkt damit der Gefahr von Entscheidungen entgegen, die auf unsachlichen Erwägungen gründen, mithin willkürlich sind.[6] Er dient sowohl der objektiven Rechtssicherheit als auch dem Schutz der Bürgerinnen und Bürger. Der demokratische Vorbehalt des Gesetzes sichert die hinreichende Legitimation und ist im Demokratiegebot (Art. 20 Abs. 2 GG) verankert.

Der Vorbehalt des Gesetzes trifft insoweit nicht nur Aussagen darüber, ob ein bestimmter Regelungsgegenstand *überhaupt* gesetzlich zu regeln ist. Er ist vielmehr auch maßgeblich für die Frage der jeweils gebotenen Regelungsdichte.[7] Die Anforderungen an die Bestimmtheit einer Ermächtigung sind umso höher, je empfindlicher grundrechtlich geschützte Freiheitsentfaltung beschränkt wird.[8] Der Gesetzgeber hat bei der Verwendung unbestimmter Rechtsbegriffe die Grundsätze der Normenklarheit und Justiziabilität zu beachten.[9] Die Reichweite des Vorbehalts des Gesetzes hängt nach der Rechtsprechung zudem von der jeweiligen „Eigenart des zu regelnden Sachverhalts“[10] bzw. von der konkreten und kontextbezogenen Funktion des Gesetzes im

---

[4] *Gärditz*, in: Friauf/Höfling (Hrsg.), Berliner Kommentar zum GG, Stand: 2020, Art. 20 Abs. 3 (Rechtsstaat) Rn. 131.

[5] BVerfGE 40, 237 (248); 49, 89 (126); 48, 210 (221); 107, 59 (102); BVerwGE 109, 29 (37).

[6] Vgl. BVerfGE 33, 125 (158).

[7] BVerfGE 8, 274 (325); 49, 89 (129); 56, 1 (13); 57, 295 (327); 83, 130 (152); 95, 267 (307 f.); 101, 1 (34).

[8] BVerfGE 48, 210 (222); 56, 1 (13); BVerwGE 90, 359 (363); 96, 189 (195).

[9] BVerfGE 8, 274 (325); 13, 153 (160 f.); 21, 73 (79); 34, 165 (192); 63, 312 (324); 78, 214 (226).

[10] BVerfGE 101, 1 (35).

Lichte der Gewaltengliederung[11] ab. Der Gesetzgeber ist verpflichtet, seine Regelungen so bestimmt zu halten, wie dies „nach der Eigenart der zu ordnenden Lebenssachverhalte und mit Rücksicht auf den Normzweck möglich ist“[12]. Dies hängt auch davon ab, „in welchem Umfang der zu regelnde Sachbereich einer genaueren begrifflichen Umschreibung überhaupt zugänglich ist“.[13] Die funktionelle Differenzierung der Staatsgewalt (Art. 20 Abs. 2 Satz 2 GG) zielt zudem auch darauf, dass „staatliche Entscheidungen möglichst richtig, das heißt von Organen getroffen werden, die dafür nach ihrer Organisation, Zusammensetzung, Funktion und Verfahrensweise über die besten Voraussetzungen verfügen“.[14] Hieraus ergeben sich auch Grenzen der Regelbarkeit, die wiederum den Vorbehalt des Gesetzes unter funktionalen Gesichtspunkten begrenzen.

Gemessen hieran ergibt sich für die Regelung des § 9b BSIG-E Folgendes:

1. Demokratische Wesentlichkeitsdoktrin

Nach ständiger Rechtsprechung hat der parlamentarische Gesetzgeber in grundlegenden normativen Bereichen, zumal im Bereich der Grundrechtsausübung alle wesentlichen Entscheidungen selbst zu treffen und darf diese nicht der Verwaltung überlassen.[15] Wesentlich sind vor allem Entscheidungen, die die Grundrechte betreffen (Grundrechtswesentlichkeit)[16]. Entscheidungen über die Grenzen der Freiheit des Bürgers dürfen nicht einseitig in das Ermessen der Verwaltung gelegt werden.

2. Folgerung 1: Wesentlich?

Ist die Verwendung von Kritischen Komponenten in TK-Netzen gemessen hieran eine wesentliche Entscheidung?

Auf den ersten Blick mag dies wie Anforderungen an die technische Sicherheit wirken, die gerade im Technikrecht eher durch Rechtsverordnungen, oft sogar nur in Verwaltungsvorschriften geregelt sind. Tatsächlich geht es jedoch vorliegend um die fundamentale Frage, auf welcher freiheitsermöglichenden Infrastruktur die elektronische Kommunikation innerhalb der Bundesrepublik Deutschland künftig stattfinden soll. Die TK-Netze sind unter den heutigen gesellschaftlichen Rahmenbedingungen das Rückgrat des öffentlichen Lebens und der individuellen Freiheit. Von Sicherheitsrisiken innerhalb der Netze betroffen wären insbesondere folgende Kernbereiche des gesellschaftlich-politischen Lebens:

- Alle *Kommunikationsgrundrechte* (insbesondere Art. 5 Abs. 1, Abs. 3, 10 Abs. 1 GG) sind beeinträchtigt, wenn individuelle Kommunikation entweder gestört oder insbesondere über abhängige Technikanbieter einem autoritären Regime zugänglich gemacht wird. Wer potentiell mit Nachteilen rechnen muss, wird sein Kommunikationsverhalten anpassen, was eine erhebliche Beeinträchtigung von Freiheit darstellt.[17] Dies gilt insbesondere dann, wenn ein mächtiger Akteur über seinen technischen Einfluss auf die Kommunikationsnetze eine hinreichend substantielle Wissensherrschaft erlangt, die er etwa gegen politische Opposition oder unliebsame Außenwahrnehmung einsetzen kann. Insoweit greifen

---

[11] BVerfGE 58, 257 (271); 68, 1 (98).

[12] BVerfGE 49, 168 (181); 59, 104 (114).

[13] BVerfGE 56, 1 (13).

[14] BVerfGE 68, 1 (86 f.); 95, 1(15); 98, 218 (252).

[15] BVerfGE 49, 89 (126 f.); 80, 124 (132); 83, 130 (142, 151 f.); 84, 212 (226); 88, 103 (116); 98, 218 (251); 101, 1 (34).

[16] BVerfGE 40, 237 (249); 47, 46 (79); 49, 89 (126 f.); 80, 124 (132); 95, 267 (307 f.); 101, 1 (34); 108, 282 (311); 116, 24 (58); 128, 282 (317); 134, 141 (184); 141, 143 (170 f.); 147, 253 (309 ff.).

[17] Vgl. BVerfGE 100, 313 (359); 120, 274 (323).

grundrechtliche Schutzpflichten für eine hinreichende Kommunikationssicherheit ein,[18] die auch den Gesetzgeber binden (Art. 1 Abs. 3 GG).

- Risiken für die Vertraulichkeit von Interaktionen berühren zudem das *Allgemeine Persönlichkeitsrecht* (Art. 2 Abs. 1 i. V. mit Art. 1 Abs. 1 GG).
- Möglichkeiten der Wirtschaftsspionage berühren die *Berufsfreiheit* und das *Eigentum* (Art. 12 Abs. 1, 14 Abs. 1 GG).
- Bei *Kritischen Infrastrukturen* hängen auch vitale Grundrechte (Art. 2 Abs. 2 Satz 1 GG), die sozialstaatliche Sicherheit (Art. 20 Abs. 1 GG) und die Vertrauenswürdigkeit des Staates von funktionierenden und hinreichend manipulationssicheren Kommunikationsinfrastrukturen ab.
- Mindestens ebenso betroffen ist die durch Art. 20 Abs. 2-3 GG gewährleistete und für einen demokratischen Rechtsstaat indisponible *Funktionstüchtigkeit demokratischer und rechtsstaatlicher Institutionen*, die untergraben wird, wenn über Kritische Komponenten des TK-Netzes Angriffe auf die demokratische Willensbildung, die innere und äußere Sicherheit oder die Vertraulichkeit von Staatsgeheimnissen erfolgen.
- Hinzu kommt, dass es überhaupt nicht zu einem tatsächlichen Angriff kommen muss. Schon die *hinreichende Möglichkeit*, technische Komponenten, die in die TK-Netze eingebaut werden, zu Manipulation zu missbrauchen, beeinträchtigt individuelle Freiheit und demokratische Institutionen. So wird bei vertraulichen Inhalten nicht nur das Kommunikationsverhalten dem nicht beherrschbaren Risiko angepasst. Demokratische Willensbildung wird vielmehr auch dadurch ganz allgemein beeinträchtigt, dass jederzeit die plausible Möglichkeit besteht (und öffentlich politisiert werden kann), etwas sei manipuliert worden. Unsicherheiten belasten so die Vertrauenswürdigkeit und Verlässlichkeit sowohl der Volks- als auch der Staatswillensbildung. Die außenpolitische Willensbildung kann im Extremfall sogar zu inadäquater Rücksichtnahme gezwungen sein, wenn (nicht beweisbarer, aber faktisch ausübbarer) Einfluss auf die TK-Netze schlicht erpressbar macht.

Zudem greift auch hier die abwehrgrundrechtliche Wesentlichkeit: § 9b Abs. 1-2 BSIG-E legt Unternehmen Handlungspflichten auf, die ihre Berufsausübungsfreiheit (Art. 12 Abs. 1 GG) beschränken und ggf. dazu führen, auf die technische leistungsstärkste und/oder günstigste Technologie verzichten zu müssen, wenn diese nicht vertrauenswürdig einsetzbar ist. § 9b Abs. 3 BSIG-E enthält zudem eine Verbotsmöglichkeit, die gegenüber den Unternehmen, die die Infrastruktur betreiben, ebenfalls unmittelbar grundrechtsrelevant ist.

Die grundlegenden Entscheidungen, welche basalen Anforderungen an die technische Sicherheit von TK-Netzen zu stellen sind, sind daher wesentlich im Sinne der bundesverfassungsgerichtlichen Rechtsprechung. Delegationsfähig wären nur akzessorische Fragen der schlichten technischen Umsetzung, die einer gesetzlichen Regelung praktisch ohnehin kaum zugänglich sind.

3. Folgerung 2: Angemessene Regelungsdichte?

Enthält gemessen hieran der Regelungsentwurf des § 9b BSIG-E eine hinreichend dichte Regelung?

Das Bundesministerium des Innern, für Bau und Heimat (im Folgenden: BMI) legt nach § 9b Abs. 2 Satz 5 BSIG-E die Mindestanforderungen für die Garantieerklärung im Einvernehmen mit den betroffenen Ressorts unter Berücksichtigung überwiegender öffentlicher Interessen, insbesondere sicherheitspolitischer Belange, durch Allgemeinverfügung (also Verwaltungsakt nach § 35 Satz 2 VwVfG) fest, die im Bundesanzeiger bekannt zu machen ist. Das Verwendungsverbot

[18] S. nur *Hoffmann-Riem*, AöR 134 (2009), 513 ff.; *ders.*, AöR 137 (2012), 509 ff.; *ders.*, JZ 2014, 53 ff.

bei fehlender oder unvollständiger Garantieerklärung nach Satz 1 gilt erst ab der Bekanntmachung dieser Allgemeinverfügung (§ 9b Abs. 2 Satz 6 BSIG).

Dies genügt aus den folgenden Gründen nicht den dargestellten Anforderungen an den Vorbehalt des Gesetzes:

- Die Regelung sieht ein Outsourcing wesentlicher Festlegungen in eine schlichte Allgemeinverfügung vor (§ 9b Abs. 2 Satz 5 BSIG): Wesentliche Fragen, welche Anforderungen Netzkomponenten grundsätzlich zu genügen haben, dürfen aber nicht *erstmals* in einem Verwaltungsakt festgelegt werden. Das Gesetz müsste zumindest die grundlegenden Parameter fixieren, was durch technische Standards zu gewährleisten ist, welchen Sicherheitszielen die Regelung dienen soll (z. B. „nur" technische Sicherheit oder auch politische Unabhängigkeit/Wehrhaftigkeit). Das Gesetz müsste auch in irgendeiner Form den normativen Grad der Erwartung an die Leistungsfähigkeit umschreiben. Jede Technik ist anfällig für Manipulation, absolute Sicherheit kann es natürlich auch hier nicht geben. Die Frage, welches Maß an Manipulationssicherheit für Kritische Infrastrukturen und Kritisch Komponenten gelten soll, müsste aber normativ auf abstrakt-genereller Ebene zumindest rahmenartig festgelegt werden. Hierzu enthält das gesamte Gesetz keine konkreten Aussagen, die über das vage Ziel des § 9b Abs. 2 Satz 4 BSIG-E hinausgehen. Das Gesetz lässt auch nicht klar erkennen, inwiefern Komponenten ausgeschlossen sein sollen, die zwar für sich den Anforderungen des Satzes 4 genügen, aber im komplexen Zusammenspiel zu Risiken führen.
- Die normativen Parameter, welche Inhalte die maßgebliche Allgemeinverfügung haben soll, bleiben völlig unklar und legen die Prioritätensetzung letztlich vollständig in die Hand der Bundesregierung. Diese gestaltet den Verwaltungsakt „unter Berücksichtigung überwiegender öffentlicher Interessen, insbesondere sicherheitspolitischer Belange" (§ 9b Abs. 2 Satz 5 BSIG-E). Die Regelung lässt der Regierung völlige Freiheit, die Infrastrukturpolitik zu beliebigen Zwecken einzusetzen. Es fehlt nicht nur eine gesetzliche Gewichtung der ggf. konkurrierenden Interessen. Das Gesetz legt nicht einmal fest, um welche öffentlichen Interessen es konkret gehen darf bzw. soll, was aber Mindestbedingung wäre, damit eine pflichtgemäße Ermessenausübung entsprechend dem Normzweck nach § 40 VwVfG normativ determiniert und kontrollierbar möglich ist. Die konstitutive Einbindung aller Ressorts („Einvernehmen") legt es letztlich nahe, dass *sämtliche* Ressortinteressen berücksichtigungsfähig sind und sich ggf. durchsetzen. Das sind dann völlig disparate und mitunter offen konkurrierende Ziele jenseits der Regelungsstrukturen des vorliegenden Gesetzes; Anhaltspunkte, wie das BMI sein Ermessen auszuüben hat, lassen sich daher der vorliegenden Regelung nicht entnehmen. Dies unterläuft aber elementare rechtsstaatliche wie demokratische Anforderungen an die Programmierung der Verwaltung.
- Insbesondere entscheidet die Regierung nach Belieben, ob und inwieweit sie die öffentlichen Sicherheitsinteressen (und damit zugleich die Freiheit der demokratischen Willensbildung sowie praktische Grundrechtsvoraussetzungen) zu Gunsten (ggf. kurzfristiger) wirtschaftlicher Interessen zurückstellt. Etwa der außenpolitische Wunsch, mit dem Staat, in dem das die fragliche Komponente herstellende Unternehmen angesiedelt ist oder von dem es beherrscht wird, ein Wirtschaftsabkommen zu schließen, eine große Investition eines deutschen Unternehmens zu begünstigen oder einen globalpolitischen Deal einzufädeln, kann willkürlich als Argument missbraucht werden, die innere und äußere Sicherheit zurückzustellen.
- Die gleiche – völlig unbestimmte – Formulierung der Ermessenziele taucht erneut in der Untersagungsermächtigung in § 9b Abs. 3 BSIG-E auf. Ob sie hier das Gleiche bedeutet, ist nicht erkennbar. Die Systematik von Zulassung (Abs. 2) einerseits und Verbot (Abs. 3) andererseits legt es jedenfalls nahe, dass darunter auch ganz unterschiedliche öffentliche

> Interessen gemeint sein können. Die ohnehin verfassungswidrige Unbestimmtheit potenziert sich, weil sich die Regierung bei einem Verbot ggf. von ganz anderen politischen Erwägungen leiten lassen kann als bei der Definition der Sicherheitsstandards.

Die zentrale Aufgabe des Gesetzgebers, politische Wertungskonflikte aufzulösen und in normativ verbindliche sowie demokratisch verantwortbare Regeln zu übersetzen, wird durch die Regelung des § 9b Abs. 2-3 BSIG-E daher im Ergebnis unterlaufen. Folgen davon sind

- ein eklatanter Verlust parlamentarischer Verantwortlichkeit der Regierung, die hier durch konturenloses Blankett ermächtigt wird, ggf. nach tagespolitischer Opportunität außerhalb politischer Verfahren der Rechtsetzung Verwaltungsentscheidungen zu treffen, und
- ein vollständiger Verlust der rechtsstaatlichen Kontrollierbarkeit, weil das Gesetz keinerlei Maßstäbe konkretisiert, nach denen Sicherheit zu gewährleisten ist.

Der Regelungsentwurf ist folglich verfassungswidrig.

II. Effektiver Rechtsschutz

Die Unbestimmtheit der materiellen Maßstäbe des § 9b BSIG-E wirft zudem die Frage auf, ob hierdurch nicht zugleich betroffenen Unternehmen (seien es die Anbieter oder Wettbewerber) effektiver Rechtsschutz abgeschnitten wird.

Art. 19 Abs. 4 GG garantiert nicht nur, dass überhaupt Rechtsschutz eröffnet ist, sondern dass dieser auch effektiv ist.[19] Das Gebot effektiven Rechtsschutzes nach Art. 19 Abs. 4 GG schließt es zwar nicht aus, „dass durch den Gesetzgeber eröffnete Gestaltungs-, Ermessens- und Beurteilungsspielräume sowie die Tatbestandswirkung von Exekutivakten die Durchführung der Rechtskontrolle durch die Gerichte einschränken."[20] Der Gesetzgeber ist bei der Einräumung von Letztentscheidungsrechten der Exekutive durch die Grundrechte sowie durch das Rechtsstaats- und das Demokratieprinzip und die hieraus folgenden Grundsätze der Bestimmtheit und Normenklarheit gebunden.

> „Will er im Übrigen gegenüber von ihm anerkannten subjektiven Rechten die gerichtliche Kontrolle zurücknehmen, hat er zu berücksichtigen, dass im gewaltenteilenden Staat grundgesetzlicher Prägung die letztverbindliche Normauslegung und auch die Kontrolle der Rechtsanwendung im Einzelfall grundsätzlich den Gerichten vorbehalten ist. Deren durch Art. 19 Abs. 4 Satz 1 GG garantierte Effektivität darf auch der Gesetzgeber nicht durch zu zahlreiche oder weitgreifende Beurteilungsspielräume für ganze Sachbereiche oder gar Rechtsgebiete aushebeln. Die Freistellung der Rechtsanwendung von gerichtlicher Kontrolle bedarf stets eines hinreichend gewichtigen, am Grundsatz eines wirksamen Rechtsschutzes ausgerichteten Sachgrunds."[21]

Hier werden durch die offene Tatbestands- und Rechtsfolgenstruktur des § 9b BSIG-E jedoch faktisch die Mindestbedingungen einer wirksamen gerichtlichen Kontrolle unterlaufen, weil kein transparenter gesetzlicher Maßstab besteht, der eine wirksame Kontrolle der durch Verwaltungsakt festgesetzten Parameter Kritischer Komponenten oder einer Untersagung im Einzelfall ermöglicht. Der Verweis auf politische Interessen ermöglicht nicht nur Willkür, sondern bezweckt diese sogar, weil bewusst kontrollierbare Maßstäbe vorenthalten werden, um es der Regierung zu

---

[19] BVerfGE 40, 272 (275); 55, 349 (369); 60, 253 (269); 113, 273 (310); 116, 1 (18); 129, 1 (20 ff.).

[20] BVerfGE 129, 1 (21 f.).

[21] BVerfGE 129, 1 (22 f.).

ermöglichen, den Grad der Sicherheit nach tagespolitischer Opportunität im Rahmen eines konturenlosen Gestaltungsermessens selbst zu bestimmen.

Mangels hinreichender Maßstäbe, nach denen das BMI die fraglichen Verwaltungsakte erlässt, wird eine wirksame Kontrolle, ob die an Kritische Komponenten angelegten Kriterien rechtmäßig sind, faktisch unterlaufen. Die Regelung verletzt daher auch Art. 19 Abs. 4 GG.

III. Inkohärenz

Daneben weist die Regelung erhebliche Kohärenzdefizite auf, die dazu führen, dass eine wirksame Anwendung jedenfalls erheblich erschwert wird. Auf folgende Punkte darf hier stellvertretend für zahlreiche Defizite hingewiesen werden:

- *Anwendungsbereich*. § 9b BSIG-E bezieht sich auf Kritische Komponenten, für die eine gesetzliche Zertifizierungspflicht besteht. Auf den ersten Blick erscheint es, als ob die Norm einen weitreichenden Schutz etabliert. Genauer besehen erweist sich die Vorschrift aber in erheblichen Teilen als erst noch auffüllungsbedürftiges Blankett. Hierzu muss die Definition des § 2 Abs. 13 Satz 2 BSIG-E in den Blick genommen werden. Ob etwas Kritische Komponente ist, hängt hiernach von einer vorherigen gesetzlichen Festlegung ab, die das vorliegende Gesetz überhaupt nicht vornimmt. Für TK-Infrastrukturen ergibt sich eine Teilregelung erst – reichlich versteckt – aus § 109 Abs. 6 TKG,[22] was sich im Übrigen nicht aus dem BSIG-E selbst, sondern erst aus seiner Begründung[23] ergibt. Die Zertifizierungspflicht wiederum ergibt sich erst aus dem mit Verweisungen überladenen und unübersichtlichen Regelungsrahmen des Gesetzes (vgl. § 9a BSIG-E).
- *Ressortübergreifendes Einvernehmen und Frist*: Die maßgebliche Allgemeinverfügung nach § 9a Abs. 2 Satz 5 BSIG-E kann das BMI nur im Einvernehmen mit den anderen Ressorts treffen. Auch ein Verbot der Verwendung von Kritischen Komponenten, die nicht hinreichend sicher sind, kann nach § 9b Abs. 3 BSIG-E nur im Einvernehmen mit allen Ressorts erfolgen. Erfolgt das Verbot nicht innerhalb eines Monats, bleibt die Verwendung zulässig. Dies bedeutet, dass selbst bei positiv festgestellten Sicherheitsrisiken das BMI innerhalb eines Montas eine einvernehmliche Entscheidung der Regierung herbeiführen muss, den Einsatz einer bestimmten Komponente zu verbieten. Damit ist die Untersagungsregelung faktisch unbrauchbar gemacht: Zunächst muss eine technisch höchst komplizierte sowie politisch sensible Frage innerhalb eines Monats entscheidungsreif gemacht werden, was schon eine große Herausforderung ist. Wenn das BMI ein Verbot befürwortet, müssen ebenfalls innerhalb der Frist alle Ressorts zur Zustimmung bewegt werden, was – nicht zuletzt in einer Koalitionsregierung – auch offene Ziel- und Wertungskonflikte einschließen kann. Am Ende kann ein einziges Ressort eine Untersagung verhindern, indem es die Zustimmung verweigert, ohne hierfür Sachgründe zu benötigen oder

[22] „Die Bundesnetzagentur erstellt im Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik und dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit einen Katalog von Sicherheitsanforderungen für das Betreiben von Telekommunikations- und Datenverarbeitungssystemen sowie für die Verarbeitung personenbezogener Daten als Grundlage für das Sicherheitskonzept nach Absatz 4 und für die zu treffenden technischen Vorkehrungen und sonstigen Maßnahmen nach den Absätzen 1 und 2. Sie gibt den Herstellern, den Verbänden der Betreiber öffentlicher Telekommunikationsnetze und den Verbänden der Anbieter öffentlich zugänglicher Telekommunikationsdienste Gelegenheit zur Stellungnahme. Der Katalog wird von der Bundesnetzagentur veröffentlicht".

[23] BT-Drs. 19/26106, S. 56.

sich – weil die innere Willensbildung der Regierung einer Ausforschung entzogen bleibt[24] – gegenüber dem Bundestag verantworten zu müssen. Eine solche dysfunktionale Regelung hat keine Vorbilder (namentlich kann auch nicht auf das gegenständlich entfernt verwandte Außenwirtschaftsrecht und die §§ 4, 13 AWG, §§ 55 ff. AWV verwiesen werden[25]) und sollte grundlegend überarbeitet werden. Wenn eine ressortübergreifende Einbindung gewollt sein sollte, würde auch ein einfacher Kabinettsbeschluss genügen, der mit Mehrheit ergeht, zumal sich das Kabinett ohnehin im Rahmen des Art. 65 GG ressortübergreifender Entscheidungen annehmen kann.

- Bei *wiederholter Feststellung nicht vorliegender Vertrauenswürdigkeit* nach § 9b Abs. 5 Nr. 1 bis 3 BSIG-E kann das BMI nach § 9b Abs. 7 BSIG-E im Einvernehmen mit den betroffenen Ressorts den Einsatz aller kritischen Komponenten des Herstellers untersagen. Es ist bizarr, dass es erst zu wiederholten (!) Verstößen gegen elementare Sicherheitsanforderungen kommen muss, damit ein Hersteller generell ausgeschlossen werden kann. Jedes Unternehmen kann es also zumindest einmal versuchen, mit einer falschen Erklärung durchzukommen. Die Sicherheitsgewährleistung bleibt hier in einem kritischen Bereich selbst hinter dem allgemeinen Gewerberecht zurück, nachdem ein unzuverlässiges Unternehmen längst seine Zulassung verloren hätte.

- Sollte überhaupt noch Anwendungsraum für die Regelung verbleiben, wird dieser durch das *inadäquate Beweismaß* endgültig beseitigt. Nach § 9b Abs. 5 Nr. 2 BSIG-E ist ein Hersteller erst dann nicht vertrauenswürdig, wenn die Erklärung *unwahre* „Tatsachen“[26] enthält. Nach allgemeinen Regeln liegt daher zugleich die Beweislast beim Bund; dieser muss also ggf. positiv inadäquate Risiken durch fremde Staaten und deren abhängige Akteure beweisen. Dies ist aus mehrerlei Hinsicht aber praktisch kaum möglich. So werden zahlreiche Erkenntnisse über *politische* Missbrauchsrisiken nicht aus der Technologie selbst allein ableitbar sein, sondern sich zumindest auch auf nachrichtendienstliche Aufklärung (namentlich durch den BND, ggf. auch durch das BfV) stützen. Diese Erkenntnisse sind aber strukturell nicht auf förmliche Beweisführung zugeschnitten. Nachrichtendienstliche Aufklärung führt zudem nur zu probabilistischen Wahrscheinlichkeitsurteilen, die eine vertretbare Prognose erlauben, erreicht aber durchweg keinen Wahrscheinlichkeitsgrad, der eine Überzeugung von der Wahrheit über jeden vernünftigen Zweifel erlaubt. Das ist auch weder die Funktion nachrichtendienstlicher Aufklärung noch von Gefahrenabwehr. Letztlich ist das normative Programm hier nicht als sicherheitspolitische Risikoabwägung

---

[24] Hierzu näher BVerfGE 67, 100 (139); 124, 78 (120 ff.); 124, 161 (189); *Geis*, in: Isensee/Kirchhof (Hrsg.), HStR III, 3. Aufl. (2005) § 55 Rn. 51; *Scholz*, AöR 105 (1980), 564 (598); *Schulte* Jura 2003, 505 (509); *Teubner*, Untersuchungs- und Eingriffsrechte privatgerichteter Untersuchungsausschüsse, 2009, S. 379 f.

[25] Schon dem Gegenstand nach unterscheiden sich unter sicherheitspolitischen Auspizien die bloße Investition in ein Unternehmen als Anteilseigner am Kapital einerseits und die Integration begrenzt transparenter ausländischer Technik in deutsche Infrastrukturen andererseits entscheiden. Die nach § 59 AWV iVm § 14a Abs. 1 Nr. 2 AWG greifende Frist zur Intervention beträgt vier Monate. Das ist schon ein gewaltiger Unterschied, wenn es darum geht, insbesondere entscheidungsunwillige Ressorts einzubinden. Die Anforderung einer Untersagung nach § 59 Abs. 1 AWV, „die öffentliche Sicherheit und Ordnung zu gewährleisten“, ist deutlich niedriger als in § 9b BSIG-E. Die AWV orientiert sich hier am Polizeirecht, verlangt also nicht mehr als eine Gefahrenprognose und verweist sogar auf die öffentliche Ordnung, also eine denkbar offene Auffangkategorie. Man vgl. zudem die Schwelle des § 60 Abs. 1b AWV. Schon der Zweck des § 4 Abs. 2 AWG ist wesentlich offener und sicherheitsfreundlicher ausgestaltet. § 13 Abs. 3 Satz 1 AWG sieht für Untersagungen die Zustimmung der Bundesregierung als Kollegialorgan vor. Diese entscheidet aber grundsätzlich im Einklang mit Art. 65 GG durch Mehrheit. Das ist etwas anderes als ein Einvernehmen mit allen Ressorts. Eine Genehmigungsfiktion der Unbedenklichkeitsbescheinigung (zwei Monate!) wird nach § 58 Abs. 2 AWV bereits dadurch verhindert, dass das BMWi ein Prüfverfahren einleitet. Das ist also eine verfahrensrechtliche Vor-Prüffrist, im BSIG-E ist es eine (halb so lange) Entscheidungsfrist.

[26] Das ist schon terminologisch ungenau, weil eine Tatsache nicht unwahr sein kann, sondern allenfalls eine Behauptung von Tatsachen.

konzipiert, die sie eigentlich ermöglichen sollte, sondern wie eine Bestimmung des Gewerberechts, in dem der Staat den gewerbefreien Bürgerinnen und Bürgern deren Unzuverlässigkeit positiv nachweisen muss.

- Die Notwendigkeit eines positiven Nachweises in § 9b Abs. 5 Nr. 2 BSIG-E birgt zudem beträchtliches *außenpolitisches Eskalationspotential*. Diese Norm verhindert es, eine Komponente einfach zurückzuweisen, weil die Verwendungssicherheit im TK-Netz (negativ) nicht hinreichend gewährleistet ist. Vielmehr muss ggf. (positiv) eine sicherheitsgefährdende Einflussnahme fremder Staaten nachgewiesen und belegt werden. Ein gesichtswahrender Rückzug ist dann nicht mehr möglich, die Anwendung der Norm treibt das BMI (und im Kielwasser die Bundesregierung) in eine direkte außenpolitische Konfrontation. Da das nicht ernsthaft intendiert sein wird, liegt ein anderer Schluss näher: Niemand hat die Absicht, auf der Grundlage des § 9b BSIG-E künftig die Nutzung Kritischer Komponenten zu untersagen.
- Soweit nachträglich *Änderungen der Allgemeinverfügung* nach § 9b Abs. 2 Satz 5 BSIG-E erfolgen, sind diese für bereits nach diesem Absatz abgegebene Garantieerklärungen unbeachtlich (§ 9b Abs. 2 Satz 7 BSIG). Das bedeutet, dass das BMI, selbst wenn es später zu neuen Erkenntnissen über Sicherheitsrisiken gelangt, die mangelnde Verlässlichkeit einer Komponente erst mit Wirkung für künftige Verfahren verwenden kann. Das ist absurd, zumal wenn später hochgradig sicherheitsgefährdende Risiken einer Komponente positiv festgestellt werden, man deren Verwendung dann aber ggf. sehendes Auges weiter dulden muss, weil bereits vorher (unterstellt: nicht vorsätzlich falsche) Garantierklärungen angegeben worden sind.

Die Summation dieser gravierenden regulativen Defizite wird absehbar dazu führen, dass der Bestimmung des § 9b BSIG-E keine relevante Bedeutung zukommen wird. Technologiebasierte Sicherheitsrisiken beim Netzausbau lassen sich jedenfalls auf dieser Grundlage nicht angemessen reduzieren. Es liegt der Verdacht nahe, dass genau das auch intendiert ist, die Regierung mit dem Entwurf des § 9b BSIG-E also nur ein Placebo in den Deutschen Bundestag eingebracht hat, um sicherheitspolitische Handlungsbereitschaft zu suggerieren, die tatsächlich gar nicht besteht, was man aber nicht transparent machen möchte.

IV. Infrastrukturgewährleistung

Insoweit bestehen auch Zweifel, ob diese bewusste Inkaufnahme von substantiellen Sicherheitslücken in den Telekommunikationsnetzen, die das Nervensystem einer modernen Gesellschaft ausmachen, dem Infrastrukturgewährleistungsauftrag aus Art. 87f Abs. 1 GG gerecht wird.

Art. 87f Abs. 2 Satz 1 GG enthält zwar zunächst eine materielle Systementscheidung für eine Leistungserbringung im Wettbewerb.[27] Das Wettbewerbsprinzip wird aber durch den in Art. 87f Abs. 1 GG niedergelegten[28] staatlichen Infrastrukturgewährleistungsauftrag überlagert.[29] „Eine Auslegung des Art. 87f Abs. 2 GG, die ausnahmslos auf die Schaffung von Wettbewerb hinausläuft, wird vom Grundgesetz unter keinem rechtlichen Gesichtspunkt gestützt.“[30] Insoweit ist

[27] BVerwGE 114, 160 (168 f.); *Möstl*, in: Maunz/Dürig (Begr.), GG, Art. 87f Rn. 38; *Remmert*, in: Epping/Hillgruber (Hrsg.), GG, 2. Aufl. (2013), Art. 87f Rn. 7; *Windthorst*, in: Sachs (Hrsg.), GG, 8. Aufl. (2018), Art. 87f Rn. 27a.

[28] BVerfGE 130, 52 (71 f.).

[29] BVerfGE 108, 370 (393).

[30] BVerfGE 108, 370 (393).

eine praktische Konkordanz zwischen den konfligierenden Zielen herzustellen.[31] Diese Bestimmung definiert die Grenzen des Privatwirtschaftlichkeitsgebots,[32] ist also spezifischer Rechtfertigungsgrund für Eingriffe in den Wettbewerb. Namentlich die grundsätzliche unternehmerische Leistungsbereitstellung im Wettbewerb (Infrastrukturwettbewerb eingeschlossen) wird also durch hoheitliche Direktiven dort eingeschränkt, wo anderenfalls der Infrastrukturgewährleistungsauftrag nicht erfüllt würde, etwa weil marktexterne politische Ziele der Netzsicherheit sichergestellt werden sollen.

Art. 87f Abs. 1 GG enthält zwar kein Optimierungsgebot, sondern einen bloßen Grundversorgungsauftrag im Sinne eines Untermaßverbots.[33] Dies verdeutlicht bereits die amtliche Begründung der Grundgesetzänderung, durch die Art. 87f GG eingeführt wurde: Der staatliche Handlungsauftrag sei „nicht auf den Ausbau einer optimalen Infrastruktur ausgerichtet, sondern zielt auf die Gewährleistung einer flächendeckenden Grundversorgung durch Sicherung der aus Sicht der Benutzer angemessenen und ausreichenden Dienstleistungen".[34] Eine „Unterversorgung der Bevölkerung mit den entsprechenden Dienstleistungen"[35] ist aber nicht erst dann gegeben, wenn Gebiete vom TK-Netz abgeschnitten oder Netzleistungen (etwa Bandbreite, Kapazität, kontinuierliche Bereitstellung) unzureichend sind. Der Infrastrukturauftrag wird vielmehr auch dann verletzt, wenn die Infrastrukturen gemessen an ihrer Funktion, kommunikative Freiheit zu ermöglichen, nicht hinreichend sicher sind. Insoweit schließt Art. 87f Abs. 1 GG eine objektiv-rechtliche Schutzverantwortung ein, TK-Netze auch gegen Angriffe, Spionage, Überwachung und Missbrauch durch Akteure zu schützen, die von fremden Staaten gesteuert werden. Ein manipulierbares oder exogenem Zugriff zugängliches Netz ist keine adäquate Infrastruktur im Sinne des Art. 87f Abs. 1 GG.

Indem § 9b BSIG-E auf konkrete und bekannte Risiken im Bereich Kritischer Komponenten mit einem faktischen Verzicht auf wirksame Abwehrmaßnahmen reagiert, unterläuft der Bund seinen aus Art. 87f Abs. 1 GG folgenden Auftrag, für sichere und verlässliche Netzstrukturen zu sorgen.

V. Notifikation

Sollte es im parlamentarischen Verfahren zu einer Änderung des Entwurfs kommen, könnte eine Notifikation gemäß Art. 5 der Richtlinie (EU) 2015/1535 des Europäischen Parlaments und des Rates vom 9. September 2015 über ein Informationsverfahren auf dem Gebiet der technischen Vorschriften und der Vorschriften für die Dienste der Informationsgesellschaft (ABl. L 241 vom 17.9.2015, S. 1) auch noch nachträglich erfolgen. Eine solche Nach-Notifikation sollte allerdings jedenfalls rein vorsorglich erfolgen. Es bestehen allerdings erhebliche Zweifel, ob eine bloße Änderung des Untersagungsverfahrens nach § 9b BSIG-E tatsächlich der Notifikation bedürfte. Denn diese Regelung betrifft nicht die anzuwenden technischen Spezifikationen oder Vorschriften, die ein auf dem TK-Binnenmarkt tätiger Hersteller einzuhalten hat, sondern lediglich die Rechtsfolgen einer Nichteinhaltung. Diese sind aber nicht unmittelbarer Gegenstand des Regelausschussverfahrens nach Art. 2 f. der Richtlinie.

---

[31] *Gersdorf*, WiVerw 2010, 150 (160); *Mayen*, in: Friauf/Höfling (Hrsg.), Berliner Kommentar zum GG, Art. 87f Rn. 207; *Möstl*, in: Maunz/Dürig (Begr.), GG, Art. 87f Rn. 38-40.

[32] *Mayen*, in: Friauf/Höfling (Hrsg.), Berliner Kommentar zum GG, Stand: 2016, Art. 87f Rn. 206.

[33] *Mayen*, in: Friauf/Höfling (Hrsg.), Berliner Kommentar zum GG, Stand: 2016, Art. 87f Rn. 139 ff.; *Möstl*, in: Maunz/Dürig (Begr.), GG, Art. 87f Rn. 65.

[34] BT-Drs. 12/7269, S. 5.

[35] BVerfGE 130, 52 (72).

VI. Gesamtwürdigung

Der Deutsche Bundestag büßt an Glaubwürdigkeit ein, wenn einerseits – mit Recht – immer wieder der verfassungsrechtlich hohe Rang der inneren und äußeren Sicherheit betont wird und hiermit verbundene Grundrechtseingriffe gerechtfertigt werden (wie zuletzt im Zuge des BNDG-Novelle in diesem Ausschuss), hier aber das Gesetz mit allen Mittel versucht, sicherheitspolitische Belange abzuwehren bzw. auszuhebeln. Bei der Regelung des § 9b BSIG-E handelt es sich letztlich um ein wirtschaftspolitisches Netz-Sicherheitsverhinderungsinstrument.

Die Regelung des § 9b BSIG-E reduziert die Frage der Nutzung Kritischer Komponenten zudem dysfunktional auf ein reines Technikproblem. Es sollen allenfalls technische Risiken eingedämmt werden. Die einer entsprechenden technologiepolitischen Entscheidung inhärente *politische* Komponente wird aber bewusst ausgeblendet. Dabei betreffen weitreichende Zukunftsentscheidungen, die in diesem Fall nachhaltigen Einfluss auf unsere Kommunikationsstrukturen und damit das freiheitliche Miteinander in unserer Gesellschaft haben werden, immer auch Fragen der Wertorientierung innerhalb der Sicherheits- und Außenpolitik. Insoweit ist es eben nicht gleichgültig, wer eine ökonomisch-technisch leistungsstarke Technologie unter welchen Bedingungen, zu welchen Zwecken und unter welchem politischen System herstellt.[36] Technologien verbinden auch Gesellschaften und insoweit lässt sich die Frage der Techniknutzung eben nicht von den Ideologien dienen, die hinter den Herstellern letztlich stehen und die um globalpolitische Macht ringen. Die rein technikbezogene Regelung des § 9b BSIG-E zielt hingegen gerade darauf ab, jedwede wertorientierte Politisierung zu verhindern und Technologiepolitik auf eine reine Marktfrage zu kondensieren. Das mag für die techniknutzenden Unternehmen adäquat sein. Freiheitliche Wertorientierung in der Technologie- und Außenpolitik, die sich natürlich nicht zwingend durchsetzen muss, aber von vornherein eine gesetzliche Absage zu erteilen, ist aber für die den Entwurf tragende Bundesregierung ein kapitulatives Armutszeugnis.

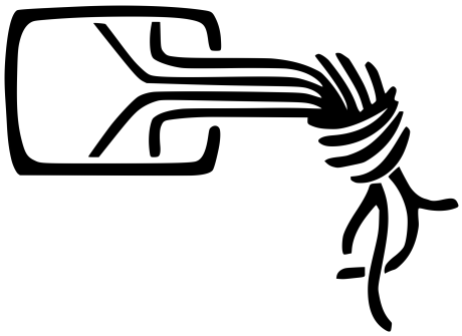
(Professor Dr. Klaus Gärditz)

[36] Der gegenwärtige Regelungsentwurf ließe es beispielsweise sogar zu, dass Komponenten eingesetzt werden, die der Hersteller durch Kinder- oder Sklavenarbeit oder durch internierte Zwangsarbeiter hergestellt hat.

Deutscher Bundestag

Ausschuss für Inneres und Heimat

Ausschussdrucksache
19(4)741 F



Sicherheit gestalten statt Unsicherheit verwalten

Sachverständigenauskunft zum Entwurf eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme

Linus Neumann

Frank Rieger, Dirk Engling, Matthias Marx

Chaos Computer Club

01. März 2021

1. Einordnung 4
1.1 Das erste IT-Sicherheitsgesetz war ein Schuss in den Ofen. 4
Das BSI verwaltet Missstände, statt ihnen aktiv entgegen zu treten. 5
Fehler sind nicht vergebens, wenn man aus ihnen lernt. 7
1.2 Anforderungen an ein zeitgemäßes IT-Sicherheitsgesetz 9
Auch ein digitales Entwicklungsland muss sich *weiterentwickeln.* 9
IT-Sicherheit *gestalten* statt verwalten! 12
Schwachstellen schließen, Sicherheitsniveau erhöhen! 13
Bürokratie ist Feindin der IT-Sicherheit. 13
Vertrauen ist gut, Kontrolle ist besser! 14
Überprüfung eigener Infrastruktur ermutigen statt kriminalisieren! 16
1.3 Einbettung in sonstige Vorhaben im Bereich der IT-Sicherheit 17
Ausweitung des Einsatzes von staatlicher Schadsoftware 17
Automatisierter Angriff auf die Vertraulichkeit von Messenger-Kommunikation 21
ZITIS: Behörde mit dem erklärten Ziel der Schwächung von IT-Sicherheit 22
Angriff auf Kommunikationsnetze durch den BND 22
Fazit 24
2. Kritik am vorliegenden Entwurf 25
Vertrauensverlust durch zweifelhaften Umgang mit Schwachstellen 25
Unwirtschaftliche und zweifelhafte Befugnis zu Portscans (§ 7b) 26
Wirtschaftlichkeit 26
Unrealistische Ziele 26
“Überwiegende Sicherheitsinteressen” 27
Überbordende Befugnisse zum Eingriff in IT-Systeme (§7c) 29
Unklare Grenzen der Anordnungsbefugnis 29
„Sinkholing“ ist schon heute gängige Praxis 29
Eingriff in die Vertraulichkeit und Integrität informationstechnischer Systeme 30
Fazit 32
Definition “vertrauenswürdiger Anbieter” greift ins Leere (§ 9b) 33
Beweise liegen nicht vor 33
Vorliegende Beweise werden ignoriert 33
Bugdoors 34
Realistische Angriffe richten sich gegen Vertraulichkeit 35
Integration von Netzwerkkomponenten 37
Technologische Souveränität 38

Konsequenzen für Betreiberinnen 39
Fazit 39
Ressourcenverschwendung durch „IT-Sicherheitskennzeichen“ (§ 9c) 40
Wirtschaftsförderungsmaßnahme ohne Realweltkonsequenzen 40
Fehlende Überprüfung 40
Alternativen 41
Falscher Fokus auf “Unternehmen im besonderen öffentlichen Interesse” 42
Abschließende Bemerkungen 44

1. Einordnung

Dem vorliegenden Gesetzentwurf kann nicht ohne den Kontext vorangegangener und paralleler Gesetzgebungsvorhaben Rechnung getragen werden.

1.1 Das erste IT-Sicherheitsgesetz war ein Schuss in den Ofen.

Das erste IT-Sicherheitsgesetz[1] wurde 2015 diskutiert und verabschiedet. In seiner damaligen Sachverständigenauskunft an den Innenausschuss des Deutschen Bundestags kritisierte der Chaos Computer Club (CCC)[2]

- fehlende Ansätze zum Schutz von Endnutzerinnen,
- Steigerung der Bürokratie statt aktiver Erhöhung der IT-Sicherheit,
- Verwässerung der Sicherheitsstandards durch Vorschlagsrecht der Betreiber,
- höhere Risiken durch geschwächten Datenschutz und
- das Vertrauensproblem des BSI durch seine fehlende Unabhängigkeit vom BMI.

Das Fazit des CCC lautete:

> *Keiner der in diesem Gesetzentwurf vorgesehenen Schritte ist geeignet, zu einer sinnvollen **Erhöhung der IT-Sicherheit** in Deutschland beizutragen. Die Auskunfts-, Dokumentations- und Berichtspflichten, die Unternehmen auferlegt werden sollen, erhöhen im Gegenteil den **Bürokratieaufwand** und gehen daher **zulasten von Ressourcen**, die andernfalls für **pro-aktive Maßnahmen** zur tatsächlichen Erhöhung der IT-Sicherheit verwendet werden könnten.*

Mit Blick auf das tägliche Angriffsgeschehen und die resultierenden Schäden für Bürgerinnen und Wirtschaft stellen wir fest, dass unsere Befürchtungen eingetreten sind.

---

[1] Bundesanzeiger: Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) vom 17. Juli 2015

[2] CCC: Stellungnahme zum Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme - IT-Sicherheitsgesetz – Linus Neumann, 17. April 2015

Das BSI verwaltet Missstände, statt ihnen aktiv entgegen zu treten.

Ein Bundesamt für Sicherheit in der Informationstechnik (BSI) muss sich daran messen lassen, dass es aktiv auf eine Erhöhung der IT-Sicherheit hinwirkt. Die durch das erste IT-Sicherheitsgesetz mandatierten Aufgaben legen den Schwerpunkt jedoch in der bürokratischen Verwaltung von Schwachstellen.

Beispiel Wahlsoftware

Vor der Bundestagswahl 2017 enthüllte der CCC eklatante Sicherheitsmängel in den zur Auswertung der Wahl verwendeten IT-Systemen, insbesondere auch einer weit verbreiteten Software zur Erfassung und Aggregation der Stimmen.[3] Zuvor hatte sich die Öffentlichkeit über Monate vor einem Hackerangriff auf die Bundestagswahl gesorgt.

Die vom CCC veröffentlichten Schwachstellen ermöglichten ein mit geringem Aufwand zu realisierendes und verheerendes Angriffsszenario auf Bundestagswahlergebnisse in mehreren Ländern. BMI und BSI zeigten sich hilflos: Rechtliche Beschränkungen hinderten das BSI am beherzten Eingriff zur Absicherung der antiken Systeme. Auch eine rechtzeitige eigenständige Untersuchung der Wahlsysteme war offenbar außerhalb des Vorstellbaren gewesen.

Es folgten mehrere inkompetente und nicht zielführende Versuche der Herstellerin, die Schwachstellen zu beheben. Schließlich “spendete” der CCC den Fix zu Behebung der schwerwiegendsten Schwachstelle.[4]

Die darauffolgenden Aktivitäten des BSI im hochkritischen Bereich der Wahlsicherheit bestanden in der Formulierung von 18 Anforderungen[5] zur Absicherung von Schnellmeldungen für die Durchführung der Europawahl 2019[6] sowie eines Anforderungskatalogs für die Bundestagswahl 2021, der zeitnah veröffentlicht werden

---

[3] ccc.de: Software zur Auswertung der Bundestagswahl unsicher und angreifbar

[4] ccc.de: Open-Source-Spende: CCC schließt größte Schwachstelle in PC-Wahl

[5] insidas.de: Europawahl 2019: Wie Kommunen die Wahlergebnisse schützen sollten, abgerufen am 26. Februar 2021

[6] bsi.bund.de: Die Lage der IT-Sicherheit in Deutschland 2019

soll. Die Anforderungen richten sich dabei an einen üblichen IT-Verbund, in dem die mangelhafte Software betrieben werden soll, zu deren Verbesserung seit 2017 offenbar kein nennenswerter Beitrag geleistet wurde:

Ende 2020 präsentierten Sicherheitsforscher auf der Jahresabschlusskonferenz des CCC[7] eklatante Schwachstellen in einer Wahlsoftware, die von der Herstellerin auch heute noch mit vollmundigen Versprechen beworben wird:

> *Bei der Entwicklung von OK.VOTE wurde höchster Wert auf das Thema Sicherheit gelegt. Diese orientiert sich an den* ***Vorgaben des Bundesamtes für Sicherheit in der Informationstechnik (BSI)*** *und der Non-Profit-Organisation Open Web Application Security Project (OWASP). Mit dem Einsatz von OK.VOTE in unserem* ***BSI-zertifizierten Outsourcing-Rechenzentrum*** *ist die Einhaltung der geforderten hohen Sicherheitsstandards gewährleistet.*[8]

Dieses Desaster zeigt abermals die Hilflosigkeit des BSI: Es ist gezwungen, Missstände zu verwalten, statt ihnen aktiv, kompromisslos und entschieden entgegentreten zu können.

Beispiel Ransomware

Kurz nach Verabschiedung des ersten IT-Sicherheitsgesetzes nahm der weltweite Trend zu Ransomware-Angriffen in Deutschland Fahrt auf: Im Jahr 2016 dominierte die Ransomware Locky[9] erstmals das Nachrichtengeschehen. In den Folgejahren konnten BSI und Bundesrepublik den Trend hilflos weiter beobachten:

- Im *Bundeslagebild Cybercrime 2016* stellt das BKA eine Zunahme um +94,4% fest,[10]

---

[7] media.ccc.de: Madl, Tobias & Obermaier, Johannes (2020): Hacking German Elections Insecure Electronic Vote Counting - How It Returned and Why You Don't Even Know About It

[8] akdb.de: OK.VOTE: Die IT-Lösung für die optimale Organisation, Vorbereitung und Durchführung von Wahlen, abgerufen am 26. Februar 2020

[9] Wikipedia: Locky

[10] BKA: Bundeslagebild Cybercrime 2016

- im *Bericht zur Lage der IT-Sicherheit in Deutschland* stellte das BSI fest, dass Ransomware "auch 2017 die maßgebliche Quelle für Schadprogramminfektionen geblieben" sei, [11]
- für das Jahr 2018 bemerkt das BKA, dass sich die "Ransomware-Szene durch eine zunehmende Professionalisierung auszeichne" [12] und
- auch im aktuellen *Bundeslagebild Cybercrime 2019* bleibt "Ransomware die größte Bedrohung für Wirtschaftsunternehmen"[13].

Während diese Gefahr über nunmehr fünf Jahre unverändert blieb, konnte in deutschen kritischen Infrastrukturen und Unternehmen nur sehr zögerlich Resilienz gegen derartige Angriffe aufgebaut werden. Dies geschah jedoch nicht wegen, sondern eher trotz des ersten IT-Sicherheitsgesetzes, dessen Untauglichkeit sich nicht nur in diesem eingängigen Beispiel illustrieren lässt.

Entsprechend nimmt auch die Problem- und Zieldefinition des vorliegenden Gesetzentwurfes (Drucksache 19/26106 in der Version vom 15.01.2021) direkt auf diese Angriffsklasse Bezug:

> *Die Schadsoftware „Emotet" dominiert bereits seit Jahren die Gefährdungslage. Vorfälle wie die Ransomware „WannaCry" verdeutlichen die Situation.*

Fehler sind nicht vergebens, wenn man aus ihnen lernt.

Es wäre natürlich wünschenswert, derartige Phänomene kritisch zu evaluieren, um mit einem zweiten IT-Sicherheitsgesetz pro-aktiv die IT-Sicherheit von morgen gestalten und künftig auf neue Trends im Angriffsgeschehen reagieren zu können. Eine Evaluation sollte natürlich nicht auf Basis anekdotischer Evidenz, sondern durch eine unabhängige und objektive Analyse erfolgen. Eine solche ist tatsächlich im ersten IT-Sicherheitsgesetz verankert, wurde jedoch von der Bundesregierung ignoriert. [14]

---

[11] BSI: Die Lage der IT-Sicherheit in Deutschland 2017

[12] BKA: Bundeslagebild Cybercrime 2018

[13] BKA: Bundeslagebild Cybercrime 2019

[14] Bundesanzeiger: Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) vom 17. Juli 2015

Insbesondere sollten die Maßnahmen zur Benennung und Regulierung der IT-Sicherheit von kritischen Infrastrukturen durch das BSI von unabhängigen Sachverständigen evaluiert werden.

Es ist bedauerlich, dass eine unabhängige Evaluation nicht erfolgt ist. Verwunderlich ist dies insbesondere, weil der vorliegende Gesetzentwurf laut Angabe der Autorinnen erstens "auf Erfahrungen mit der Anwendung der im ersten IT-Sicherheitsgesetz geregelten Befugnisse" basieren und zweitens die Regulierungsbefugnisse des BSI erheblich erweitern soll.

Empfehlung: Die Bundesregierung sollte gesetzeskonform zunächst die Evaluation des ersten IT-Sicherheitsgesetzes durchführen. Auf Basis dieser Evaluation könnte ein empirisch gestütztes IT-Sicherheitsgesetz Fehler des ersten IT-Sicherheitsgesetzes korrigieren.

1.2 Anforderungen an ein zeitgemäßes IT-Sicherheitsgesetz

Ziel eines *Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme* sollte die Erhöhung der Sicherheit informationstechnischer Systeme sein. Einleitend ist festzuhalten, dass es sich bei der IT-Sicherheit um einen zumindest theoretisch relativ fortgeschrittenen Forschungsbereich handelt: Alle *praktisch relevanten* Probleme sind *theoretisch* gelöst. Es gibt zurzeit keine essentiellen praktisch relevanten Herausforderungen, deren theoretische Lösung unbekannt wäre. Trotzdem ist der Zustand der IT-Sicherheit in der Praxis desaströs.

Dies liegt einerseits an der mangelnden Umsetzung von technischem Basiswissen der IT-Sicherheit, andererseits an den Herausforderungen der organisatorischen IT-Sicherheit und der Mensch-Maschine-Interaktion. Jeder IT-Sicherheitsvorfall – ob klein, ob groß – lässt sich auf die Verletzung wohlbekannter Regeln und Prinzipien der IT-Sicherheit zurückführen. Das lapidar klingende Ziel muss sein, dass diese in der Breite auch kompromisslose Anwendung finden. Dass dieses Ziel zurzeit in weiter Ferne scheint, zeigt nur, wie dringend es verfolgt werden muss und wie eklatant es in den vergangenen Jahrzehnten vernachlässigt wurde.

Statt vorhandene Ressourcen zu nutzen und auszubauen, versucht das BMI, das Rad auf Basis der Quadratur des Kreises neu zu erfinden: Systeme sollen einerseits unsicher genug sein, dass Strafverfolgungsbehörden und Geheimdienste eindringen können, andererseits sollen Wirtschaft und Bürgerinnen auf „sichere“ IT vertrauen können. Dieser janusköpfige Ansatz ist zum Scheitern verurteilt.

Auch ein digitales Entwicklungsland muss sich *weiterentwickeln.*

Die Herausforderungen der SARS-CoV-2-Pandemie haben deutschen Bürgerinnen die mangelhafte digitale Infrastruktur und die daraus resultierende mangelnde Digitalisierung relevanter Lebens- und Wirtschaftsbereiche schmerzlich spüren lassen.

Die Bundesrepublik hat in den vergangenen Jahrzehnten zu jedem Zeitpunkt über die finanziellen Ressourcen verfügt, durch mutige Investition, Förderung und Bildung zur digitalen Vorzeigenation ausgebaut zu werden. Entsprechende Vorstöße waren jedoch immer halbherzig, wurden nicht zu Ende gedacht und kaputt-bürokratisiert, bevor sie ihr Potenzial entfalten konnten.

Zaghafte Ansätze im Bereich der IT-Sicherheit ereilte das gleiche Schicksal. Die *De-Mail*, das *besondere elektronische Anwaltspostfach* und der *elektronische Personalausweis* sind nur einige Beispiele für Projekte, die sich zur Geißel aller Beteiligten oder zu mahnenden Bauruinen mit Nutzungszahlen im hohen einstelligen Bereich entwickelten. Die Ursache war in allen Fällen die gleiche: Eine fehlende Strategie, um kompromisslos und mutig Digitalisierung und IT-Sicherheit einen Schritt voran zu bringen.

Auch in der Digitalisierung der Verwaltung fehlte jegliche Strategie – und wo es an einer Strategie mangelt, steht früher oder später die Konsolidierung ins Haus. Im Jahre 2015 erstmals groß angekündigt, hat diese bisher das dreifache Budget verschlungen, ohne dass ein Ende in Sicht wäre.[15] [16] Das Versagen hat System.

Und genau dieses System und dieses Versagen sind dafür verantwortlich, dass die Bundesrepublik sich ohne Einflussmöglichkeiten als Spielball im Feld der IT-Sicherheit bewegt, statt das Feld aktiv zu gestalten. So sieht dieses System aus:

[15] tagesschau.de: IT-Projekt des Bundes: 3,4 Milliarden Euro und kein Ende, abgerufen am 26. Februar 2021

[16] spiegel.de: Modernisierung der Bundes-IT: Verheerende Zwischenbilanz, abgerufen am 26. Februar 2021

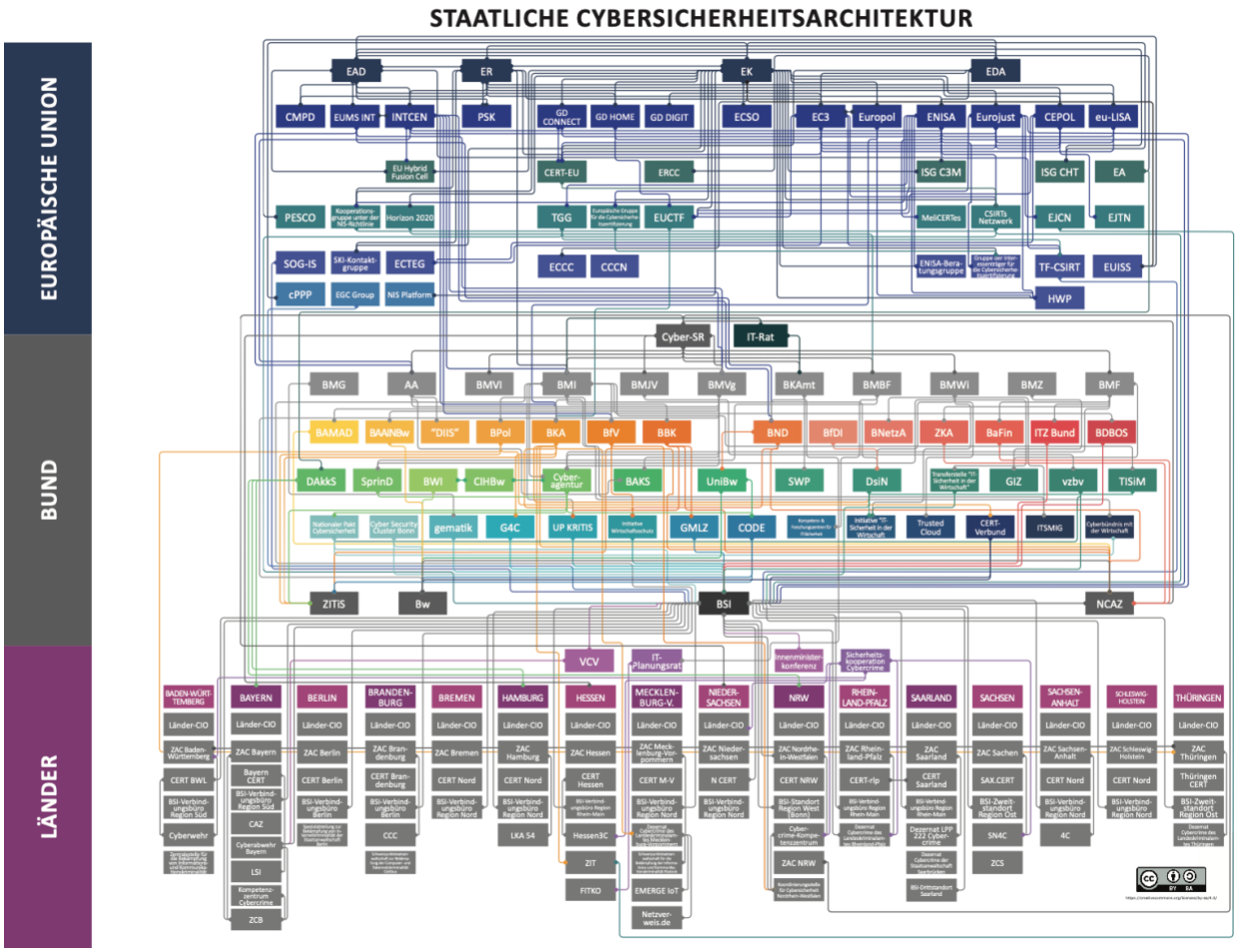


Abbildung 1. Staatliche Cybersicherheitsarchitektur. Aus: Herpig, Sven & Beigel, Rebecca (2020): Deutsche Cybersicherheits- und Cyberverteidigungspolitik: Staatliche Akteure und Zuständigkeiten (5. Auflage)[17]

Empfehlung: Der Deutsche Bundestag möge sich vom Bundesministerium des Innern, für Bau und Heimat das obige Schaubild erklären lassen oder eine Person finden, die dazu in der Lage ist.

[17] Herpig, Sven & Beigel, Rebecca (2020): Deutsche Cybersicherheits- und Cyberverteidigungspolitik: Staatliche Akteure und Zuständigkeiten (5. Auflage), zuletzt abgerufen am 26. Februar 2020. Für neue Auflagen siehe ggf. stiftung-nv.de: Akteure und Zuständigkeiten in der deutschen Cybersicherheitspolitik

Empfehlung: Die Bundes- und Länderregierungen mögen die Zuständigkeiten und Aufgaben in der deutschen IT-Sicherheitspolitik auf Interessenkonflikte, Verantwortungsdiffusion und Konsolidierungspotenziale untersuchen, Interessenkonflikte auflösen und Konsolidierungspotenziale realisieren.

IT-Sicherheit *gestalten* statt verwalten!

Es ist nicht möglich, *auch ein bisschen Digitalisierung* zu machen. Und es ist nicht möglich, *auch ein bisschen IT-Sicherheit* zu machen – vor allem *nicht nachträglich.*

Ein einzelner Brand muss gelöscht werden. Zu diesem Zweck wird es immer eine Feuerwehr geben müssen. Wenn aber die Brände in Frequenz und Anzahl die Kapazitäten jeder Feuerwehr um ein Vielfaches übersteigen, wird es Zeit, über Brandschutz nachzudenken: IT-Sicherheit muss schon beim Schreiben der ersten Zeile Code, vor dem Platzieren des ersten Elements im Netzwerk-Architekturdiagramm bedacht werden. Den Überlegungen muss ein Bedrohungsmodell zugrunde liegen und das obere Ziel muss immer die Verringerung von Angriffsfläche sein.

Werden diese Grundprinzipien nicht bedacht, verkommen nachträgliche Bemühungen zur Herstellung von IT-Sicherheit zur Sisyphos-Aufgabe. Leider müssen sich Bürgerinnen, Wirtschaft und kritische Infrastrukturen auch heute noch dieser Sisyphos-Aufgabe stellen, weil es an einer kompromisslosen IT-Sicherheitsstrategie und einer auf dieser Basis errichteten sicheren Basis mangelt.

Dass Betreiberinnen kritischer Infrastruktur auch heute meist keine andere Wahl haben, als hochkritische Komponenten mit hoffnungslos veralteten Systemen zu steuern, ist Ergebnis einer inzwischen jahrzehntelangen Strategielosigkeit, die sich im Verwalten von Schwachstellen und dem halbherzigen Ergreifen nicht abgestimmter Einzelmaßnahmen niederschlägt.

Von dieser mangelnden Strategielosigkeit und dem fehlenden Gestaltungswillen ist leider auch der vorliegende Gesetzentwurf geprägt.

IT-Sicherheit kennt keine Kompromisse.

Schwachstellen in der IT-Sicherheit kennen keine Kompromisse, kein gutes Zureden, keine Gnade und auch keine Nachsicht. Vor allem aber kennen sie nicht den Unterschied zwischen Gut und Böse. Systeme können nur entweder für alle Nutzerinnen sicher oder für alle Nutzerinnen unsicher sein.

Es wird Zeit, dass diese recht simple, aber fundamentale Erkenntnis sich auch in der IT-Sicherheitspolitik der Bundesrepublik Deutschland durchsetzt.

Empfehlung: Ein IT-Sicherheitsgesetz muss konkrete und kompromisslose Maßnahmen zur Erhöhung von IT-Sicherheit beschließen. Abwägungen und gezielte Schwächungen sind ebenso fehl am Platz wie ambitionslose Ansätze zur Verwaltung von Unsicherheit.

Schwachstellen schließen, Sicherheitsniveau erhöhen!

Seit vielen Jahren wiederholt der CCC die Forderung nach einem kompromisslosen und unabhängigen BSI. Der vorliegende Gesetzentwurf zeigt in besonderer Tragik auf, wie wichtig diese Forderung ist.

Zurückgehaltene Schwachstellen betreffen immer alle betroffenen Systeme und damit auch die des Staates, der Zivilgesellschaft, Wirtschaft und kritischen Infrastrukturen. Die mitunter katastrophalen Konsequenzen einer solchen Geheimhaltung kann man am Beispiel der Angriffe “Wannacry” und “Notpetya” sehen, die im Gesetzentwurf und seiner Begründung selbst mehrmals exemplarisch herangezogen werden.

Empfehlung: Unter keinen Umständen sollte das BSI jemals berechtigt sein, bei Kenntnis von Schwachstellen etwas anderes zu tun, als die Betroffenen zu informieren, auf eine Beseitigung hinzuarbeiten und zu gegebenem Zeitpunkt die Öffentlichkeit zu warnen.

Bürokratie ist Feindin der IT-Sicherheit.

Wenngleich sich dieser Eindruck einer Bürgerin der Bundesrepublik Deutschland vielleicht nicht unmittelbar aufdrängt, handelt es sich bei der IT und deren Sicherheit um ein sehr dynamisches Feld, in dem auch nur zeitweiser Stillstand unmittelbaren Rückschritt bedeutet.

Implizite Maßgaben wie *„never change a running system“*, denen die Annahme zugrunde liegt, ein einmal geprüftes System würde sicher bleiben, bedeuten genau diesen Rückschritt. Implizit auf solchen Maßgaben basierende Zertifizierungen und bürokratische Hürden gehen daher mit enormen Opportunitätskosten einher: Sie verhindern aktiv die Weiterentwicklung und dynamische Auseinandersetzung mit zukünftigen Herausforderungen.

Empfehlung: Ein IT-Sicherheitsgesetz sollte IT-Sicherheit fördern, statt sie durch Bürokratie auszubremsen.

Vertrauen ist gut, Kontrolle ist besser!

Im ewigen Wettlauf zwischen Angriff und Verteidigung können nur nachhaltige Sicherheitsmaßnahmen dauerhaften Vorsprung bieten. Fehlt schon das Vertrauen in eine sichere Basis, kann keine sichere Infrastruktur geschaffen werden.

Insbesondere kritische Infrastrukturen und nicht zuletzt die Einrichtungen des Bundes sind seit jeher von mangelndem Vertrauen in IT-Systeme geplagt. Möglichkeiten, eine sichere, nachhaltige und quelloffene Basis bereitzustellen, bleiben ungenutzt.

Durch die Bündelung von Ressourcen und das freie Zugänglichmachen der Ergebnisse in Open-Source-Projekten könnte die Bundesrepublik wichtige Grundlagen für nachhaltige technologische Souveränität legen.

Schaffung eines Pools von auditierter Open-Source-Software

Moderne Software und Systeme beruhen auf einer Vielzahl von Einzelkomponenten aus verschiedensten Quellen. Dabei ist die Sicherheit des Gesamtsystems höchstens so gut wie die der einzelnen Komponenten. Nicht selten handelt es sich bei sicherheitskritischen Software-Bibliotheken um von Freiwilligen in ihrer Freizeit programmierte Open-Source-Software mit stark schwankenden Sicherheitseigenschaften. Im Sinne einer nachhaltigen, dauerhaften Verbesserung der IT-Sicherheit – auch für die vom BSI direkt betreuten Behörden – ist es unerlässlich, die Sicherheit und Qualität möglichst vieler Open-Source-Komponenten dauerhaft zu steigern.

Empfehlung: Schaffung eines Pools von auditierter Open-Source-Software

1. Bereitstellung von Ressourcen für die unbürokratische und schnelle Auditierung existierender Open-Source-Komponenten.

2. Schaffung einer Organisation, die die langfristige Förderung der Entwicklung sicherer Open-Source-Software unter einer permissiven Lizenz, die auch den Einsatz in der Wirtschaft erlaubt, zum Ziel hat.

3. Unbürokratische dauerhafte Förderung von Entwicklungsprojekten für Hard- und Software-Komponenten durch diese Organisation, die bisher fehlen oder für die nur Optionen in nicht ausreichender Qualität verfügbar sind.

Nachhaltige Verbesserung der Bildung und Ausbildung im Bereich IT-Sicherheit

Ohne gut ausgebildetes Personal ist keine Verbesserung der IT-Sicherheit zu erzielen. Auch im Jahre 2021 verlassen Informatik-Absolventinnen deutsche Universitäten, ohne auch nur ein Seminar zum Thema IT-Sicherheit oder sicherem Programmieren belegt zu haben.

Empfehlung: Nachhaltige Verbesserung der Bildung und Ausbildung im Bereich IT-Sicherheit durch

1. Verpflichtende Einführung von Bildungskomponenten für die sichere Konfiguration von Systemen und Programmierung von Software in allen Bildungswegen, deren Absolventinnen IT-Systeme entwickeln (Ausbildung und Studium).

2. Bereitstellung von kostenfreiem, hochqualitativen Bildungsmaterial für IT-Sicherheit und sichere Software-Entwicklung für alle Bildungswege durch den Bund.

Überprüfung eigener Infrastruktur ermutigen statt kriminalisieren!

Zur Überprüfung der IT-Sicherheit eigener Infrastruktur gehört der regelmäßige und kontrollierte Einsatz von Angriffsprogrammen. Jedoch wird der Einsatz solcher Programme zur Erforschung ihrer Wirkweise und Folgen mit § 202c StGB kriminalisiert.[18] Dies benachteiligt den Industrie- und IT-Sicherheitsstandort Deutschland und setzt Forscherinnen, Betreiberinnen und Prüferinnen einem realitätsfremden Rechtsrisiko aus.

Empfehlung: § 202c StGB sollte gestrichen werden, um die Überprüfung eigener Infrastruktur durch den kontrollierten Einsatz von Angriffsprogrammen nicht nur ohne Rechtsrisiko zu ermöglichen, sondern auch zu ermutigen.

[18] ccc.de: § 202c StGB gefährdet den IT-Standort Deutschland

1.3 Einbettung in sonstige Vorhaben im Bereich der IT-Sicherheit

Der vorliegende Gesetzentwurf hat zum Ziel, die *"Cyber- und Informationssicherheit"* für die *"Digitalisierung aller Lebensbereiche"* zu *"gewährleisten."* Schon im ersten Absatz wird korrekt festgestellt:

> *Voraussetzung hierfür ist eine sichere Infrastruktur.*

Das Ziel einer sicheren Infrastruktur wird im vorliegenden Gesetzentwurf jedoch nur halbherzig verfolgt, in anderen Initiativen des BMI sogar aktiv verhindert.

Da die Bundesregierung in parallelen Gesetzesvorhaben und Initiativen auf EU-Ebene eine gezielte Schwächung digitaler Infrastrukturen vorantreibt, kann der vorliegende Entwurf nicht ohne diesen Kontext in Gänze bewertet werden. Im Folgenden werden daher zunächst exemplarisch gleichzeitige Bemühungen der Bundesregierung zusammengefasst, die eine Schwächung der digitalen Infrastrukturen zum erklärten Ziel haben. Aufgrund der Fülle dieser Bemühungen konzentrieren wir uns dabei ohne Anspruch auf Vollständigkeit auf die wichtigsten Vorstöße seit Inkrafttreten des ersten IT-Sicherheitsgesetzes:

Ausweitung des Einsatzes von staatlicher Schadsoftware

Die Befugnisse zum Einsatz von Schadsoftware zur Durchführung der so genannten "Quellen-Telekommunikationsüberwachung" und "Online-Durchsuchung" wurden 2017 im Rahmen der Änderung der Strafprozessordnung massiv ausgeweitet[19]. Der CCC warnte in seiner Sachverständigenauskunft an den Rechtsausschuss des Bundestags vor *Risiken für die innere Sicherheit beim Einsatz von Schadsoftware in der Strafverfolgung*[20], weil die IT-Sicherheit der Endgeräte dafür erheblich beeinträchtigt wird. Seitdem wurde die Befugnis zur Quellen-TKÜ auf insgesamt 44 Straftatbestände ausgeweitet. Mehrere Gesetzentwürfe weiten auch die Befugnis zur Online-Durchsuchung aus.

---

[19] netzpolitik.org: Wir veröffentlichen den Gesetzentwurf der Großen Koalition zum massenhaften Einsatz von Staatstrojanern, abgerufen am 26. Februar 2021

[20] ccc.de: Risiken für die innere Sicherheit beim Einsatz von Schadsoftware in der Strafverfolgung

Um diese Maßnahmen umzusetzen, werden Schwachstellen in den Systemen der Zielpersonen benötigt. Schwachstellen können jedoch nur in allen Systemen gleichzeitig vorhanden oder nicht vorhanden sein. Sie sind politisch neutral und stehen grundsätzlich allen Angreiferinnen zur Verfügung. Zwar lassen sich staatliche Hintertüren theoretisch mit wirksamem Zugriffsschutz versehen, doch diese Hintertüren ließen sich nicht geheim halten. Es wäre daher töricht anzunehmen, dass Kriminelle Geräte mit derartigen Schwachstellen und Hintertüren nutzen würden. Geschwächt bleiben deutsche Bürgerinnen und die deutsche Wirtschaft, während Kriminelle auf sichere – und obendrein potenziell illegale! – Systeme ausweichen.

Dem für diese Schwächung verantwortlichen Bundesministerium des Innern, für Bau und Heimat untersteht auch das Bundesamt für Sicherheit in der Informationstechnik, das sogar aktiv an der Entwicklung eines deutschen Staatstrojaners mitgewirkt hat.[21] Der Chaos Computer Club hat diesen Staatstrojaner 2011 analysiert und nachgewiesen, dass die verfassungsrechtlich vorgeschriebenen Grenzen der Schadsoftware in vielerlei Hinsicht weit überschritten wurden.[22]

Es stellt sich die Frage, wie das BSI mit so offensichtlichen Interessenkonflikten und zweifelhafter Vorgeschichte in Zukunft glaubwürdig zur IT-Sicherheit in Deutschland beitragen soll, solange es der Weisungsbefugnis des BMI unterliegt.

Gesetz zur Anpassung des Verfassungsschutzrechts

Um diese Schwächung der Endgeräte komfortabler vornehmen zu können, sollen mit dem *Gesetz zur Anpassung des Verfassungsschutzrechts*[23] nun sogar Netzbetreiberinnen in die Pflicht genommen werden, durch gezielte Umleitung von Internetverkehr Angriffe auf die eigenen Kundinnen zu ermöglichen. Dies ist ein katastrophaler Eingriff in das Vertrauensverhältnis zwischen Infrastrukturanbietern und Bundesbürgerinnen.

---

[21] netzpolitik.org: BSI programmierte und arbeitete aktiv am Staatstrojaner, streitet aber Zusammenarbeit ab, abgerufen am 26. Februar 2021

[22] ccc.de: Analyse einer Regierungsmalware

[23] bundestag.de Gesetz zur Anpassung des Verfassungsschutzrechts

Des Weiteren sollen neben den Strafverfolgungsbehörden auch alle 19 Geheimdienste die Befugnis zum Einsatz von Staatstrojanern erhalten.

Es ist schwer vorstellbar, wie sich diese weitreichenden Eingriffe zur Schwächung von Infrastruktur- und Kommunikationssicherheit mit dem vorliegenden Gesetzentwurf in Einklang bringen lassen sollen.

Gesetz zur Modernisierung der Rechtsgrundlagen der Bundespolizei

Mit dem geplanten *Gesetz zur Modernisierung der Rechtsgrundlagen der Bundespolizei* sollen Staatstrojaner sogar gegen Menschen eingesetzt werden dürfen, die nicht einmal einer Straftat verdächtigt werden, wenn beispielsweise angenommen wird, dass eine Person eine *Straftat in der Zukunft begehen wird*, oder *angenommen wird, dass ihr Endgerät von einer verdächtigten Person benutzt werden wird.* [24]

Auch hier führt das BMI einen kompromisslosen Kampf gegen die Vertraulichkeit der Kommunikation und damit die IT-Sicherheit der Bürgerinnen.

Kooperation mit zweifelhaften Herstellern

Das BKA ist seit 2012 Kunde des Unternehmenskonglomerats "Gamma/Finfisher",[25] gegen das sich seit Mitte 2019 strafrechtliche Ermittlungen des Zollkriminalamts richten. Auslöser für diese Ermittlungen ist eine Strafanzeige der Gesellschaft für Freiheitsrechte, Reporter ohne Grenzen, dem Europäischen Zentrum für Verfassungs- und Menschenrechte sowie netzpolitik.org. In diesem Rahmen hat auch der Chaos Computer Club eine Analyse durchgeführt, die eindeutige Hinweise für den Einsatz der Schadsoftware gegen demokratische Oppositionelle in der Türkei und somit das Umgehen von Exportrestriktionen durch das Firmenkonglomerat zusammenträgt.[26]

---

[24] bundestag.de: Gesetzentwurf der Fraktionen der CDU/CSU und SPD zum Entwurf eines Gesetzes zur Modernisierung der Rechtsgrundlagen der Bundespolizei, abgerufen am 26. Februar 2021

[25] netzpolitik.org: Bundeskriminalamt kauft international bekannten Staatstrojaner FinFisher/FinSpy von Gamma, abgerufen am 26. Februar 2021

[26] ccc.de: CCC analysiert Münchner Staatstrojaner FinSpy

Anfang Oktober 2020 wurden von der Staatsanwaltschaft München I in Zusammenarbeit mit dem Zollkriminalamt insgesamt 15 Geschäftsräume und Privatwohnungen rund um München und ein Unternehmen aus dem Umfeld des Konglomerats in Rumänien durchsucht.

Während hinsichtlich der strafbewehrten Umgehung von Exportrestriktionen bisher nur ein Verdacht besteht, der Auslöser für die umfassenden Ermittlungsmaßnahmen war, ist der weltweite, wiederholte und grobe Verstoß gegen rechtsstaatliche Prinzipien durch Gamma/Finfisher öffentlich seit Jahren über jeden Zweifel erwiesen. Ihre Produkte wurden mindestens eingesetzt:

- gegen die demokratische Opposition in Ägypten,[27]
- gegen Aktivistinnen in Bahrain,[28]
- gegen US-Bürgerinnen auf Betreiben Äthiopiens,[29]
- gegen die Opposition in Uganda,[30]
- etc. pp.

Diese Angriffe finden unter Ausnutzung menschlicher und technischer Schwachstellen seit über einem Jahrzehnt statt und werden von der Bundesregierung offenbar nicht nur nicht bekämpft, sondern das Betreiben der Unternehmensgruppe sogar durch aktive Kundschaft gefördert.

---

[27] amnesty.org: German-made FinSpy spyware found in Egypt, and Mac and Linux versions revealed, abgerufen am 26. Februar 2021

[28] privacyinternational.org: Bahraini Government, With Help From FinFisher, Tracks Activists Living In The United Kingdom, abgerufen am 26. Februar 2021

[29] citizenlab.ca: You Only Click Twice – FinFisher's Global Proliferation, abgerufen am 26. Februar 2021

[30] privacyinternational.org: Ugandan Government Deployed FinFisher Spyware To 'Crush' Opposition, Track Elected Officials And Media In Secret Operation During Post-Election Protests, Documents Reveal, abgerufen am 26. Februar 2021

Die eigentlich im Arbeitsauftrag des BSI liegenden Maßnahmen zur Bekämpfung der Schadsoftware, beispielsweise durch die öffentliche Bereitstellung von Analyse-Tools, Detektionsregeln[31] und Forschungsergebnissen[32], werden derweil vom CCC geleistet.

Vor diesem Hintergrund ist kaum verwunderlich, dass staatliche Bestrebungen scheitern, die IT-Sicherheit für Bürgerinnen und Wirtschaft zu erhöhen.

Automatisierter Angriff auf die Vertraulichkeit von Messenger-Kommunikation

Der CCC engagiert sich seit vielen Jahren für den *Ausstieg aus unverschlüsselter Kommunikation*.[33] Dieses Schutzziel teilt die Bundesregierung offenbar nicht: In einer Stellungnahme an den Innenausschuss des Bundestags 2020 musste der CCC sogar der Forderung nach einem kompromisslosen *Recht auf Verschlüsselung* Nachdruck verleihen.[34]

Das groß angekündigte Verschlüsselungsprojekt De-Mail wird inzwischen selbst von den Betreiberinnen als "überkomplizierter" und "toter Gaul" bezeichnet. Trotz Investitionen in dreistelliger Millionenhöhe habe es "nie jemanden gegeben, der dieses Produkt genutzt hat."[35] Der Chaos Computer Club hatte in mehreren Sachverständigenauskünften vor der Untauglichkeit des Systems gewarnt.[36][37]

Nachdem auch das *besondere elektronische Anwaltspostfach (beA)* gelinde gesagt suboptimale Ergebnisse hervorbrachte, sind verschlüsselte Messenger die derzeit einzige niederschwellige und massenhaft zur Verfügung stehende

---

[31] github.com: Schröder, Thorsten & Neumann, Linus (2018): FinSpy-Tools, abgerufen am 26. Februar 2021

[32] github.com: Neumann, Linus & Schröder, Thorsten (2018): FinSpy-Dokumentation, abgerufen am 26. Februar 2021

[33] ccc.de: CCC fordert Ausstieg aus verschlüsselter Kommunikation

[34] ccc.de: CCC fordert kompromissloses Recht auf Verschlüsselung

[35] Jungundnaiv.de: Tim Höttges, Vorstandsvorsitzender der Deutschen Telekom AG, "Jung und Naiv" Folge 498, abgerufen am 26. Februar 2021

[36] ccc.de: Gutachten unterstreicht Untauglichkeit der De-Mail für rechtsverbindliche Kommunikation

[37] ccc.de: Chaos Computer Club erneuert Kritik am Gesetzentwurf zur De-Mail

Verschlüsselungslösung zum Schutz deutscher Bürgerinnen und Unternehmen. Statt diesen überfälligen Zugewinn an Sicherheit zu begrüßen und zu fördern, ist das BMI stets bemüht, die gewonnene Sicherheit wieder abzubauen.

Auf EU-Ebene engagiert sich die Bundesregierung für Scanner und Filter, die Kommunikation auf illegale Inhalte prüfen sollen. Dass dabei sämtliche Kommunikationsinhalte gescannt werden, wird geflissentlich ignoriert. Um dies zu ermöglichen, sollen sogar aktiv die Anforderungen der e-Privacy-Richtlinie abgeschwächt werden,[38] weil diese derartige Scanner aktiv verbieten.

ZITIS: Behörde mit dem erklärten Ziel der Schwächung von IT-Sicherheit

Seit April 2017 unterhält das BMI eine eigene Bundesanstalt zur gezielten Schwächung der IT-Sicherheit. Zu deren vier Geschäftsfeldern gehören die Telekommunikationsüberwachung und Kryptoanalyse zum gezielten Brechen verschlüsselter Kommunikationsinhalte. Als Bedarfsträgerinnen der "Zentralen Stelle für Informationstechnik im Sicherheitsbereich" gelten BKA, BfV und BPOL, im Beirat haben weiterhin BND, MAD, ZKA und BMI Gaststatus.

Alle genannten Behörden befinden sich – ebenso wie das BSI – im Geschäftsbereich des BMI. Es bleibt unerklärlich, wie das BSI seinem Arbeitsauftrag ungehindert nachkommen soll, wenn die eigene Dienstherrin mit so ausgeprägter Verve gegenteilige Interessen verfolgt.

Angriff auf Kommunikationsnetze durch den BND

Im Mai 2020 hat das Bundesverfassungsgericht die Internetüberwachung durch den Bundesnachrichtendienst für grundgesetzwidrig erklärt. Der BND betreibt diese Überwachung seit Jahren ohne gesetzliches Mandat, welches ihm durch die BND-Gesetznovelle erstmals – gemäß dem Motto "Das Gesetz verstößt gegen den

---

[38] europa.eu: Vorschlag für eine VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES über eine vorübergehende Ausnahme von bestimmten Vorschriften der Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates hinsichtlich der Verwendung von Technik durch Anbieter nummernunabhängiger interpersoneller Kommunikationsdienste zur Verarbeitung personenbezogener und anderer Daten zwecks Bekämpfung des sexuellen Missbrauchs von Kindern im Internet, abgerufen am 26. Februar 2021

Geheimdienst" – erteilt worden war. Auch der zweite, aktuell stattfindende Versuch, ein grundgesetzkonformes BND-Gesetz zu formulieren, droht derweil an schlichter Ignoranz gegenüber dem Grundgesetz und dem Urteil des Bundesverfassungsgerichts zu scheitern.

Mit der zum Zeitpunkt des Schreibens dieser Stellungnahme noch nicht beschlossenen Novelle des BND-Gesetzes soll der BND ermächtigt werden, ohne Wissen der jeweiligen Betreiberin auf Bestands-, Verkehrs- und Inhaltsdaten zuzugreifen und hierzu *mit heimlichen Mitteln und/oder unter Zugriff auf informationstechnische Systeme von Telekommunikationsanbietern Sicherungsmaßnahmen zu überwinden*.[39] Damit werden alle Diensteanbieterinnen von Telekommunikation, Clouddiensten und sonstigen Telemediendiensten im Ausland erklärte Ziele staatlichen Hackings.[40][41]

Diese aktive Ermächtigung zum Angriff auf die Vertraulichkeit internationaler Kommunikationsnetze und deren Betreiberinnen ist insbesondere im Hinblick auf den geplanten *§ 9b (2) Untersagung des Einsatzes kritischer Komponenten* relevant. Siehe hierzu *Definition "vertrauenswürdiger Anbieter" greift ins Leere (§ 9b)*, Seite 33.

---

[39] bundestag.de: Entwurf eines Gesetzes zur Änderung des BND-Gesetzes zur Umsetzung der Vorgaben des Bundesverfassungsgerichts sowie des Bundesverwaltungsgerichts in der Version vom 25. Januar 2021, abgerufen am 26. Februar 2021

[40] netzpolitik.org: BND-Gesetz: Sachverständige kritisieren Hacken und Ausspähen unter Freunden, abgerufen am 26. Februar 2021

[41] netzpolitik.org: BND-Gesetz: Eine neue Lizenz zum Hacken, abgerufen am 26. Februar 2021

Fazit

Die Bundesregierung verwendet mehr Energie auf den gezielten Abbau von IT-Sicherheit als auf ihre aktive Förderung. Dieses Engagement steht im diametralen Gegensatz zum Schutzbedarf der deutschen Bürgerinnen und der Wirtschaft der Bundesrepublik Deutschland.

Empfehlung: Bundestag und Bundesregierung sollten IT-Sicherheit zum konkreten und kompromisslosen Ziel der Innenpolitik der Bundesrepublik Deutschland machen und dieses Ziel auch aktiv verfolgen.

Bestrebungen zur Schwächung der IT-Sicherheit von Endgeräten und digitalen Infrastrukturen sind umgehend einzustellen.

Bereits erlassene Gesetze zur Schwächung der IT-Sicherheit von Endgeräten und digitalen Infrastrukturen sind entsprechend zu revidieren.

2. Kritik am vorliegenden Entwurf

Im Folgenden werden ausgewählte Aspekte des vorliegenden Gesetzentwurfs einer eingehenden Bewertung unterzogen. Grundsätzlich ist hervorzuheben, dass dem BSI in seiner aktuellen organisatorischen Einbindung aufgrund des offensichtlichen Interessenkonflikts mit der Dienstherrin keinerlei Befugnisse zum aktiven Eingreifen in IT-Systeme oder zur Sammlung sensibler Daten gewährt werden sollten.

Empfehlung: Das BSI muss als eigenständige und unabhängige Bundesbehörde aus dem Aufsichtsbereich des BMI herausgelöst werden, um seinem gesetzmäßigen Auftrag kompromisslos nachgehen zu können.

Siehe hierzu insbesondere auch *"Überwiegende Sicherheitsinteressen"*, Seite 27.

Vertrauensverlust durch zweifelhaften Umgang mit Schwachstellen

Der vorliegende Gesetzentwurf räumt dem BSI weitreichende Kompetenzen ein, hochsensibles Wissen über kritische Schwachstellen zu erlangen und anzuwenden. Mittels automatisierter Scanner soll das BSI nicht nur nach Schwachstellen suchen, sondern auch mittels *Brute-Force*-Angriffen aktiv unberechtigten Zugriff auf Systeme anstreben.

Im Sinne der Verteidigung gehören derartige Angriffsversuche zum Standardrepertoire der IT-Sicherheit: Schwachstellen werden gefunden, um sie zu schließen. Der vorliegende Gesetzentwurf versäumt aber, das BSI zur Einhaltung minimaler ethischer Standards der IT-Sicherheitsforschung zu verpflichten. Stattdessen wird das BSI explizit zur Verletzung ethischer Standards ermächtigt: Breitflächige Ausnahmetatbestände sollen es dem BSI erlauben, entgegen seinem erklärten Auftrag Schwachstellen *nicht* zu melden, betroffene IT-Systeme *wissentlich* unsicher zu lassen und aktive Angriffe wissentlich *zu ermöglichen, statt sie zu verhindern*.

Empfehlung: Unter keinen Umständen sollte das BSI jemals berechtigt sein, bei Kenntnis von Schwachstellen etwas anderes zu tun, als die Betroffenen zu informieren, auf eine Beseitigung hinzuarbeiten und zu gegebenem Zeitpunkt die Öffentlichkeit zu warnen.

Unwirtschaftliche und zweifelhafte Befugnis zu Portscans (§ 7b)

Mit *„§7b Detektion von Sicherheitsrisiken für die Netz- und IT-Sicherheit und von Angriffsmethoden“* soll dem BSI die Befugnis eingeräumt werden, mittels Portscans vorher bestimmte informationstechnische Systeme *„des Bundes oder kritischer Infrastrukturen, digitaler Dienste und der Unternehmen im besonderen öffentlichen Interesse“* auf Sicherheitslücken zu prüfen.

Wirtschaftlichkeit

Der Erfüllungsaufwand wird mit einmalig 1.7 Mio. und jährlich mehr als 1.1 Mio. Euro beziffert:

> *Um diese neue Aufgabe effektiv umzusetzen, benötigt das Bundesamt 10 Planstellen/Stellen (7 hD; 3 gD) mit Personalkosten in Höhe von jährlich 0,94 Mio. Euro sowie Sacheinzelkosten in Höhe von 0,25 Mio. Euro jährlich. Zusätzlich wird mit einmaligen Sachkosten in Höhe von 1,7 Mio. Euro gerechnet.*

Es ist zutreffend, dass es sich bei Portscans *um ein Verfahren handelt, das grundsätzlich jedermann zugänglich ist und das regelmäßig auch zu Angriffszwecken von Kriminellen genutzt wird*. Eine Reihe privatwirtschaftlicher Anbieterinnen führt diese bereits regelmäßig durch und stellt die Ergebnisse teils kostenlos öffentlich zur Verfügung. Tiefergehende Analysen, Suchfunktionen und Auswertungen von unterschiedlicher Qualität und Aussagekraft werden teils von unseriösen, teils von seriösen Anbieterinnen zu moderaten Preisen angeboten.

Empfehlung: Im Rahmen der Wirtschaftlichkeit sollte das BSI die bestehenden kommerziellen Angebote hinsichtlich ihrer Aussagekraft evaluieren.

Unrealistische Ziele

Der Kreis der potenziellen Ziele für Portscans durch das BSI ist eng gewählt und deckt Privatanschlüsse und KMU nicht mit ab. Dadurch wird zumindest sichergestellt, dass die Empfängerinnen der Portscans von ihrem Glück wissen, in Zukunft neben den vielen täglichen Portscans auch regelmäßig das BSI in den Logfiles begrüßen zu dürfen.

Systeme, die einem Portscan nicht standhalten, werden schon das “Internet-Grundrauschen” an Angriffsaktivität nicht überleben. Zwischen den avisierten Portscans durch das BSI und dem Vorgehen von tatsächlichen Angreiferinnen gibt es

jedoch einen entscheidenden Unterschied: Angreiferinnen automatisieren nicht nur die Suche nach Schwachstellen, sondern auch deren direkte Ausnutzung.

Es ist daher höchst unwahrscheinlich, dass das BSI eine *öffentlich bekannte Schwachstelle* schneller findet, als interessierte Angreiferinnen und diese schneller melden und beheben lassen kann, als Angreiferinnen für die automatisierte Ausnutzung brauchen.

Empfehlung: Die Ressourcen des BSI sollten in aussichtsreichere Aktivitäten investiert werden, die Schwachstellen am Entstehen zu hindern.

"Überwiegende Sicherheitsinteressen"

In §7b Absatz 3 erfährt die Informationspflicht des BSI gegenüber den Betreiberinnen betroffener Geräte eine empfindliche Einschränkung:

> *Wird durch [Portscans] eine Sicherheitslücke oder ein anderes Sicherheitsrisiko eines informationstechnischen Systems erkannt und* ***stehen überwiegende Sicherheitsinteressen nicht entgegen,*** *sind die für das informationstechnische System Verantwortlichen darüber zu informieren.*

Diese Einschränkung ist ein weiteres von unzähligen Beispielen für die Unterordnung der Sicherheitsinteressen der kritischen Infrastrukturen der Bundesrepublik Deutschland gegenüber den Unsicherheitsinteressen des BMI. Es ist nicht weniger als eine durchschaubare Frechheit, Befugnisse zum Aufspüren von Sicherheitslücken zum Zwecke der Information der Betroffenen einzufordern und sich noch auf der gleichen Seite des Gesetzentwurfs von der Informationspflicht zu entbinden.

Die konkrete Motivation zur wissentlichen Geheimhaltung von Schwachstellen wird inzwischen nicht einmal mehr galant geleugnet. So betont beispielweise das BKA freimütig, dass es Kenntnis von Schwachstellen hat, diese aktiv ausnutzt, und die verantwortlichen Stellen nicht darüber in Kenntnis setzt:

Zum anderen [würden] die Anbieter kommerzieller Hard- und Software in die Lage versetzt, die von der Überwachungssoftware genutzten Angriffsvektoren (Schwachstellen etc.) zu ***schließen*** *und den Einsatz der Software unter Umständen* ***dauerhaft zu verhindern****. Dies hätte eine schwerwiegende* ***Beeinträchtigung*** *der Fähigkeiten der zuständigen Sicherheitsbehörden zur Sachverhaltsaufklärung im Rahmen der Strafverfolgung bzw. Gefahrenabwehr insbesondere in den Kriminalitätsfeldern Terrorismus/Extremismus und der Organisierten Kriminalität zur Folge.*[42] [43]

Schwachstellen werden demnach wissentlich geheim gehalten und ihre Ausnutzung durch Dritte in Kauf genommen.

Empfehlung: Unter keinen Umständen sollte das BSI jemals berechtigt sein, bei Kenntnis von Schwachstellen etwas anderes zu tun, als die Betroffenen zu informieren, auf eine Beseitigung hinzuarbeiten und zu gegebenem Zeitpunkt die Öffentlichkeit zu warnen.

[42] fragdenstaat.de: ZV 32-21-5391.04-2/18 – Widerspruchsbescheid zur Anfrage *Überprüfung von Produkten der ITÜ*, abgerufen am 26. Februar 2021

[43] netzpolitik.org: Das BKA verhindert, dass Sicherheitslücken geschlossen werden, abgerufen am 26. Februar 2021

Überbordende Befugnisse zum Eingriff in IT-Systeme (§7c)

Mit §7c soll das BSI ermächtigt werden, a) die Umleitung von Internetverkehr und b) das Versenden *„technischer Befehle zur Bereinigung von einem konkret benannten Schadprogramm an betroffene informationstechnische Systeme“* anzuordnen. Während die Umleitung von Internetverkehr schon heute gängige Praxis ist, würde mit dem aktiven Eingriff in potenziell befallene Systeme riskantes Terrain betreten. Die vorgeschlagenen rechtlichen Rahmenbedingungen sind weder dem Risiko noch dem Missbrauchspotenzial angemessen.

Unklare Grenzen der Anordnungsbefugnis

In § 7c Abs. 1 wird die Verpflichtung von Anbieterinnen im Sinne des Telekommunikationsgesetzes so unscharf definiert, dass nicht ersichtlich ist, ob auch Anbieterinnen von nicht rufnummern- oder leitungsgebundenen Telekommunikationsdiensten unter die Verpflichtung fallen.

Durch die geplante Ausweitung des Kreises der Verpflichteten im Telekommunikations-Modernisierungsgesetz entsteht hier auch eine potentielle Ausweitung der Auswirkung der Eingriffsbefugnisse auf einen weiten Kreis von Anbieterinnen mit erheblichen Konsequenzen für die Schwere des Eingriffs.

Empfehlung: Die Anordnungsbefugnis muss Anbieterinnen von nicht rufnummern- oder leitungsgebundenen Telekommunikationsdiensten, Betriebssystemen, App Stores etc. explizit *ausschließen* und darf sich nur auf Anbieterinnen von „Datenleitungen“ im engsten Sinne des Wortes beziehen.

„Sinkholing“ ist schon heute gängige Praxis

Die Befugnisse des BSI zur Anordnung eines Eingriffs in die Telekommunikation werden nicht beschränkt auf Fälle, in denen die TK-Anbieterin nicht selbst in der Lage ist, notwendige Maßnahmen zur Eindämmung von weit verbreiteten Schadprogrammen zu treffen.

Das BSI soll mit einer uneingeschränkten Befugnis ausgestattet werden, die einen unnötigen Interessens- und Verantwortungskonflikt erzeugt: Insbesondere große TK-Anbieterinnen sind bereits heute entsprechend der in § 100 9a Abs. 5 und 6 des TKG erteilten Befugnisse dazu in der Lage und auch erfolgreich beim Erreichen der

definierten Schutzziele. Die Kooperation von Unternehmen bei der Bekämpfung von Schadsoftware und Botnetzen ist ein eingespielter Prozess, in den das BSI nur eingreifen sollte, wenn er nicht funktioniert. Das BSI würde hier in einem funktionierenden und bestehenden Prozess als unnötige dritte Partei eingefügt.

Empfehlung: Die Befugnisse des BSI zur Anordnung von „Sinkholing" sollten sich auf solche Fälle beschränken, in denen TK-Anbieterinnen nicht selbst in der Lage sind, entsprechende Maßnahmen zu treffen oder umzusetzen.

Missbrauchspotenzial

Die in Abs. 2 eingeräumte Befugnis zur Umleitung von Datenverkehr ist nicht hinreichend spezifisch definiert. Die derzeitige Formulierung lässt es auch zu, Verkehr zu Servern umleiten zu lassen, die Informationen bereitstellen, die im weitesten Sinne den Schutzzielen zuwiderlaufen. Dabei wäre bei der derzeitigen Formulierung auch eine Zensur von Informationen rechtens, die nur im weitesten Sinne als schädlich für die definierten Schutzziele angesehen werden können.

Empfehlung: Eingriffe in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme müssen zumindest post-hoc durch ein unabhängiges Aufsichtsgremium geprüft werden.

Eingriff in die Vertraulichkeit und Integrität informationstechnischer Systeme

Die in § 7c Abs. 1 Satz 2 vorgeschlagene Befugnis zur Anordnung der Verbreitung *„technischer Befehle zur Bereinigung von einem konkret benannten Schadprogramm an betroffene informationstechnische Systeme"* ist vage und unzureichend definiert. Dieses Versäumnis ist von besonderer Schwere, da es sich um eine potenziell folgenschwere Ermächtigung zum Eingriff in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme[44] handelt.

Weder wird eindeutig geklärt, ob sich diese Befugnis auch auf Systeme von Kunden der betroffenen TK-Anbieterin, also hinter dem Router befindliche Computer,

[44] Wikipedia: Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme

Industrieanlagen, Krankenhaussysteme etc. erstreckt, noch wird definiert, welchen Beschränkungen diese „technischen Befehle“ unterliegen.

Dem Eingriff werden auch keine Qualitätsanforderungen zugrunde gelegt. Gleichzeitig bleibt die Haftung für eventuelle Schäden und Nebenwirkungen (z. B. Datenverlust oder Verlust der Verfügbarkeit von Systemen) ungeklärt.

Empfehlung: Eingriffe in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme müssen von eng definierten Voraussetzungen, ausführlicher Transparenz und streng eingegrenzten Zielen flankiert werden.

Die Befugnis verletzt den Verhältnismäßigkeitsgrundsatz, nach dem insbesondere bei Eingriffen in Grundrechte von möglichen Maßnahmen nur diejenige ergriffen darf, die die Betroffenen und die Allgemeinheit am wenigsten beeinträchtigt.

Empfehlung: Das Ergreifen von Maßnahmen geringerer Eingriffstiefe sollte zur Voraussetzung für einen derartigen Eingriff vorgeschrieben werden.

Wenn etwa die in Frage stehende „Schadsoftware“ nicht hinreichend gut verstanden wurde und beispielsweise verborgene Routinen zur Löschung oder Verschlüsselung von Daten des betroffenen Systems enthält, kann ein gegenüber der Ausgangssituation viel schwerwiegenderer Schaden entstehen.

Empfehlung: Die Haftungsfrage ist zu klären.

Von besonderer Schwere ist die fehlende Definition der Eigenschaften eines *„konkret benannten Schadprogramms“* zu dessen *„Bereinigung“* das BSI ermächtig werden soll: Insbesondere mit Hinblick auf die Paragraphen § 202a-c StGB würde mit § 7c ein willkürlicher Ermessenspielraum mit ausgiebigem Missbrauchspotenzial geschaffen.

Empfehlung: Der Begriff „Schadprogramm“ muss eng und konkret definiert werden, um das Missbrauchspotenzial einzugrenzen.

Mangelnde Transparenz

Der vorliegende Gesetzentwurf enthält keine Pflichten zur öffentlichen Dokumentation der eingesetzten *„technischen Befehle“*, des *„konkret benannten Schadprogramms“* oder

der betroffenen Systeme. Dadurch wird Betroffenen im Schadensfall ein Regress erheblich erschwert. Ebenso gibt es keine Möglichkeit nachzuvollziehen, ob die *„technischen Befehle“* nachvollziehbar dem proklamierten Zweck – und nur diesem – dienten.

Die Einbeziehung der Bundesnetzagentur und der Bundesbeauftragten für den Datenschutz und Informationsfreiheit ist keine ausreichende Absicherung gegen Kollateralschäden einer automatisierten Ausführung von *„technischen Befehlen“* durch das BSI auf potentiell Millionen betroffener Systeme.

Empfehlung: Eingriffe in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme müssen zumindest post-hoc durch ein unabhängiges Aufsichtsgremium geprüft werden. Das Aufsichtsgremium muss vollständigen Einblick in den Vorgang, sowie die Möglichkeit zur Sanktionierung haben.

Fazit

Die Zielsetzung, eine effektive Handlungsmöglichkeit zur zeitnahen Bekämpfung von weit verteilter Schadsoftware zu erlangen, ist nachvollziehbar. Die derzeitige vorgeschlagene Regelung ist jedoch unnötig unspezifisch und weist keine Regelung für Schadensfälle auf, die durch solche Eingriffe entstehen. Im Ergebnis bietet sie ein weit über den intendierten Anwendungszweck hinausgehendes Missbrauchspotenzial.

Grundsätzlich ist der Eingriff in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme hochkritisch und sollte nur im eng definierten absoluten Ausnahmefall als Ultima Ratio zugelassen sein. Beschränkungen oder enge Voraussetzungen wie bspw. die Verpflichtung zur vorherigen Anwendung von Maßnahmen mit geringerer Eingriffstiefe finden sich jedoch nicht im vorliegenden Gesetzentwurf.

Insbesondere vor dem Hintergrund der nach aktuellen Gesetzesvorhaben verstärkten Einbindung des BSI in den Bereich der öffentlichen Sicherheit entsteht ein umfangreicher Vertrauensverlust. Dieser macht es zwingend erforderlich, derartige Eingriffsbefugnisse mit effektiven Hürden und Kontrollmechanismen zu versehen.

Definition “vertrauenswürdiger Anbieter” greift ins Leere (§ 9b)

Die Rolle chinesischer Netzwerkausrüstungsunternehmen wird weltweit seit 2018 emotional und von Fakten weitgehend unbelastet geführt. Wir möchten einleitend unmissverständlich klarstellen, dass diese Diskussion völlig lächerlich und fehlgeleitet ist. Sie ist ein herausragendes Beispiel für die Hilflosigkeit, Strategielosigkeit und Ahnungslosigkeit der bundesdeutschen IT-Sicherheitspolitik.

Wir äußern uns hierzu nur widerwillig und mit dem primären Ziel, diese Debatte auf eine sachliche Grundlage zu stellen.

Beweise liegen nicht vor

Einen humorvollen Höhepunkt erreichte die Diskussion im März 2019, als hochrangige US-Diplomaten der Bundesregierung mit der Einstellung der Geheimdienstkooperation drohten, sofern diese beim Aufbau eines 5G-Netzes Komponenten einer chinesischen Herstellerin zulasse.[45] Ungeachtet dessen, ob eine solche Kooperation überhaupt im Interesse der Bundesbürgerinnen ist, erscheint sie doch als relativ geschmackloses Druckmittel zur Durchsetzung handelspolitischer Interessen.

Ein Beweis für die mangelnde Vertrauenswürdigkeit der genannten Herstellerin wurde der interessierten Öffentlichkeit bisher nicht präsentiert – wenngleich Medienberichten zu entnehmen ist, dass die Bundesregierung spätestens seit Beginn 2020 über einen solchen Beweis verfügen soll.[46]

Vorliegende Beweise werden ignoriert

Bisher hat die Bundesregierung jedoch keinerlei Maßnahmen unternommen, um der Verwendung entsprechender Komponenten Einhalt zu gebieten. Der Öffentlichkeit bleibt indes unbekannt, ob die von den USA präsentierten Beweise nicht glaubwürdig sind, oder schlichtweg ignoriert werden. Letzteres kommt in Betracht, weil die Bundesregierung sogar bei Herstellerinnen, deren mangelnde Vertrauenswürdigkeit

---

[45] Der Spiegel: USA stellen wegen Huawei Geheimdienst-Kooperation infrage, abgerufen am 26. Februar 2021

[46] Handelsblatt: „Smoking gun“: Streit um Beweise gegen Huawei, abgerufen am 26. Februar 2021

öffentlich unwiderlegbar dokumentiert ist, keinen Anlass zum Handeln sieht: Die Aktivitäten der US-Geheimdienste in diesem Bereich sind seit Ende 2013 öffentlich ausführlich dokumentiert,[47] [48] ohne dass die Bundesregierung daraus Konsequenzen gezogen hätte. Der bekannteste mit Hilfe dieser Infrastruktur durchgeführte Angriff auf Mitgliedstaaten der Europäischen Union ist die Infiltration des Belgacom-Netzwerks, das unter anderem die Kommunikationsinfrastruktur für das EU-Parlament in Brüssel stellt.[49] Ungeachtet der tatsächlichen Bewertung der Vertraulichkeit einer spezifischen Herstellerin ist also festzuhalten, dass derartige Angriffe auf Kommunikationsinfrastruktur stattfinden.

Eine nicht vertrauenswürdige Herstellerin könnte hierbei zumindest theoretisch eine Unterstützung leisten. Für die Herstellerin hätte dies jedoch einen potenziell sehr hohen Preis: das Ende sämtlicher internationaler Handelsbeziehungen – sofern Regierungen oder Netzbetreiberinnen auf solche Angriffe Konsequenzen folgen lassen würden.

Um der Argumentation der Autorinnen des vorliegenden Gesetzentwurfs zu folgen, sei davon ausgegangen, dass eine nicht vertrauenswürdige Herstellerin zur Beeinträchtigung der IT-Sicherheit der Kommunikationsinfrastruktur der Bundesrepublik Deutschland verpflichtet sei.

Bugdoors

Statt offensichtlich als solche gedachte Backdoors in gelieferten Systemen zu verstecken, wäre eine nicht vertrauenswürdige Anbieterin besser beraten, die gelieferten Systeme mit schwer zu entdeckenden, komplexen Schwachstellen auszustatten: Im Fall einer Entdeckung könnten diese plausibel als unbeabsichtigte Sicherheitslücken behandelt und beseitigt werden, ohne dass Zweifel an der Vertrauenswürdigkeit der Anbieterin entstünden.

---

[47] Wikipedia: NSA ANT catalog

[48] Wikipedia: Tailored Access Operations

[49] Wikipedia: Operation Socialist

Um ausgewählten staatlichen Stellen ein Ausnutzen der absichtlichen Schwachstellen zu ermöglichen, würde die nicht vertrauenswürdige Anbieterin das Wissen über diese Schwachstellen und die Möglichkeit derer Ausnutzung heimlich weitergeben.

Realistische Angriffe richten sich gegen Vertraulichkeit

Eine nicht vertrauenswürdige Anbieterin könnte grundsätzlich Schwachstellen bereitstellen, die zur Beeinträchtigung der Verfügbarkeit, Integrität oder Vertraulichkeit eines Kommunikationsnetzes geeignet sein könnten. Hier lohnt es sich, die Konsequenzen einer Ausnutzung jeweils deren Nutzen gegenüber zu stellen.

1. **Verfügbarkeit:** Das Sabotieren einer Kommunikationsinfrastruktur wäre ein kriegerischer Akt, der aufgrund der hohen Abhängigkeit vom Kommunikationssystem unvorhersehbare Schäden zur Folge haben könnte. Der Vorfall würde unmittelbar bekannt und ließe sich mit großer Wahrscheinlichkeit sowohl nachweisen als auch attribuieren. Die ökonomischen Konsequenzen für die nicht vertrauenswürdige Herstellerin wären fatal.
2. **Integrität:** Die Beeinträchtigung der Integrität des Kommunikationsnetzes könnte beispielsweise im Umlenken von Verbindungen bestehen. Ein solches hoch dynamisches Vorgehen würde einen breitbandigen Zugang zum manipulierten Ziel-Netz voraussetzen. Die Netzwerkbetreiberin hätte jedoch gute Möglichkeiten, diese Zugriffe zu erkennen und zu unterbinden, da relevante Teile der kritischen Kommunikationsinfrastrukturen nicht ungehindert über das Internet administrativ erreichbar sind.
3. **Vertraulichkeit:** Die Schwächung eines Kommunikationsnetzes zum Zweck der Spionage bietet für Angreiferinnen langfristige Vorteile bei gleichzeitig geringer Entdeckungswahrscheinlichkeit. Würde beispielsweise die Verschlüsselung auf der Luftschnittstelle geschwächt, wäre das Abhören der Netzverbindungen für Eingeweihte mit einfachen Mitteln möglich, ohne dass netzwerkseitige Auffälligkeiten zur Entdeckung führen könnten.

Vor dem Hintergrund dieser einfach nachvollziehbaren Überlegungen scheint es am wahrscheinlichsten, dass durch eine nicht vertrauenswürdige Anbieterin absichtlich platzierte Schwachstellen zum Zweck der *Vertraulichkeitsverletzung* ausgenutzt würden.

Insbesondere ist hierbei festzuhalten, dass mit der geplanten Novelle des BND-Gesetzes der Auslandsgeheimdienst der Bundesrepublik spezifisch zu solchen Angriffen ermächtigt werden soll. Die geplanten Angriffe sollen dabei ausschließlich die *Vertraulichkeit* der Kommunikationsnetze, *nicht* jedoch deren Verfügbarkeit oder Integrität beeinträchtigen.

Dieses wahrscheinlichste Angriffsszenario wird jedoch durch den vorliegenden Gesetzesvorschlag explizit ignoriert, indem nur *Verfügbarkeit und Integrität* als Schutzziele genannt werden, und die Vertraulichkeit im Gegensatz zu allen anderen Stellen im Gesetzestext, die die Schutzziele der Informationssicherheit behandeln, *ausgeklammert wird*. § 9b Abs. 5 Nr. 5 besagt:

> *Ein Hersteller einer kritischen Komponente ist nicht vertrauenswürdig, wenn […]*
> *5. die kritische Komponente über technische Eigenschaften verfügt oder verfügt hat, die geeignet sind oder waren, missbräuchlich auf die* ***Sicherheit, Integrität, Verfügbarkeit oder Funktionsfähigkeit*** *der Kritischen Infrastruktur einwirken zu können.*

Der aufmerksamen Leserin ist sicherlich nicht entgangen, dass ausgerechnet das Schutzziel der Vertraulichkeit in dieser Auflistung überraschenderweise fehlt.

Empfehlung: Die Schutzziele der Informationssicherheit sind Verfügbarkeit, Integrität und *Vertraulichkeit*.[50]

[50] wikipedia.org: Informationssicherheit

Empfehlung: Die Definition „vertrauenswürdiger Anbieterinnen" muss sich nicht auf die Herkunft der Anbieterin, sondern auf die tatsächliche und prüfbare technische Sicherheit und Sicherbarkeit ihrer Produkte erstrecken.

Alle Anbieterinnen von Komponenten kritischer Infrastruktur – unabhängig von ihrem Herkunftsland – sollten nur zulässig sein, wenn sichergestellt ist, dass das tatsächlich im Einsatz befindliche System auditiert werden kann. Entsprechende Auditierungen sollten regelmäßig stattfinden.

Die technischen Voraussetzungen (Reproducible Builds, Bereitstellung von unabhängigen Audit-Ressourcen entsprechend dem Update-Tempo, Nachweis von „Best Practices" für Mitigation in Architektur, Coding-Praxis, Build-Prozess etc.) sollten in die Anforderungen für alle Anbieterinnen aufgenommen werden.

Empfehlung: Damit es für diese Prozesse der Überprüfung vertrauenswürdig ist, darf das BSI nicht zum Dienstleister für Behörden werden, die Sicherheitslücken im Rahmen ihrer Tätigkeit zu benötigen glauben, verheimlichen und ausnutzen (BND, BfS, MAD, BKA, LKAs), da sich hierdurch ein nicht glaubwürdig auflösbarer Interessenskonflikt ergibt:

Das BSI muss ein striktes Mandat zur schnellstmöglichen Behebung aller ihm egal auf welchem Wege bekanntwerdenden Sicherheitslücken bekommen, für das keine Ausnahmen zugelassen sind.

Integration von Netzwerkomponenten

Würde eine nicht vertrauenswürdige Herstellerin zur Beihilfe bei der Beeinträchtigung der Verfügbarkeit oder Integrität von Kommunikationsnetzen verpflichtet, so ist es aus den oben genannten Gründen unwahrscheinlich, dass die Beeinträchtigung über das Internet per Mausklick auf einen großen roten Knopf ausgelöst werden könnte. Insbesondere ist dies unwahrscheinlich, weil die Komponenten in nicht öffentlich zugänglichen Netzen administriert werden.

Tatsache ist aber, dass Zulieferinnen und Dienstleisterinnen im Rahmen ihrer Tätigkeit detaillierte Kenntnis von Netzwerkarchitektur, Zugangsvoraussetzungen und Sicherheitssystemen der Kommunikationsnetze erlangen, in denen ihre Produkte eingesetzt werden. Dieses Wissen erstreckt sich auch über die Komponenten anderer Anbieterinnen im *vendor mix:* Aus naheliegenden Gründen kommt in Kommunikationsnetzen zur Vermeidung einseitiger Abhängigkeiten eine Mischung von Komponenten unterschiedlicher Hersteller zum Einsatz.

Tatsächliche Trägerinnen von sicherheitsrelevantem Wissen sind daher weniger die internationalen Produzentinnen, sondern die in Deutschland ansässigen Unternehmen, die entsprechender Jurisdiktion unterliegen.

Empfehlung: Zusätzlich zu fortlaufenden, vollständigen Sicherheits-Audits aller Netzwerk-Komponenten sollten Betreiberinnen von TK-Netzen verpflichtet werden, innerhalb ihrer Netze Systeme zur Detektion von Anomalien in der Kommunikation zwischen den verwendeten Komponenten zu betreiben. Diese sollten geeignet sein, Anzeichen für Kompromittierung durch Angreiferinnen oder eine Ausnutzung von Back- und Bugdoors zu detektieren. Auf diese Weise lassen sich unabhängig vom Herkunftsland der Herstellerinnen Angriffe und Anomalien im Betrieb erkennen.

Technologische Souveränität

Schon heute sind europäische Netzwerkkomponenten nicht in der Lage, mit chinesischen Produkten zu konkurrieren: Chinesische Anbieterinnen liefern inzwischen technisch überlegenes Equipment zu günstigeren Preisen. Es ist daher leicht nachvollziehbar, dass deutsche und europäische Mobilfunknetze zu großen Teilen mit chinesischer statt europäischer Technik ausgerüstet werden.

Unabhängig von der Frage der Vertrauenswürdigkeit der Anbieterinnen ist es im Interesse der Bundesrepublik und der Europäischen Union, die europäische Technik konkurrenzfähig im Markt zu halten. Beim Bau von Mobilfunknetzen der sechsten oder siebten Generation droht sonst eine Situation, in der europäische Ausrüster nicht mehr Teil des Angebots sind.

Um dem entgegenzuwirken, bieten sich jedoch etablierte und “ehrliche” Mittel der Marktverzerrung wie Förderungen, Subventionen und Zölle an. Es bedarf nicht eigens

des Arguments von einer in der IT-Sicherheit konzeptuell fremden "Vertrauenswürdigkeit."

Konsequenzen für Betreiberinnen

Würde eine massenhaft eingesetzte Herstellerin plötzlich als "nicht vertrauenswürdig" erkannt, wäre ein Rückbau bzw. Ersatz der verbauten Infrastruktur die zwingend logische Konsequenz.

Dieser Rückbau ginge jedoch mit erheblichen Einschränkungen und finanziellen Belastungen einher – sofern überhaupt Alternativen verfügbar sind.

Hierbei ist insbesondere zu berücksichtigen, dass schon heute deutsche Mobilfunknetze der dritten und vierten Generation zu überwiegenden Teilen aus Hardware zweier von der Bundesregierung potenziell als "nicht vertrauenswürdig" beurteilter Herstellerinnen bestehen.

Fazit

Das Konzept der *"nicht vertrauenswürdigen Anbieter"* verfehlt sein Schutzziel. Wenn der Bundesregierung Beweise für die mangelnde Vertrauenswürdigkeit einer Herstellerin vorliegen, so möge sie diese der Öffentlichkeit präsentieren und daraus Konsequenzen ziehen.

Empfehlung: Wenn es der Bundesregierung daran gelegen ist, die technologische Souveränität im Bereich des Mobilfunks aufrecht zu erhalten, dann möge sie mit Förderprogrammen die mangelnde Konkurrenzfähigkeit europäischer Herstellerinnen kompensieren. Hierzu bieten sich breit angelegte Programme zur Förderung von kritischen Software-Stacks als Open-Source an, für die im Rahmen der Förderung auch die Ressourcen für sichere Architekturen und fortlaufende Auditierung bereitgestellt werden.

Ressourcenverschwendung durch „IT-Sicherheitskennzeichen“ (§ 9c)

Besonders offiziell erscheinende IT-Sicherheitskennzeichen wünschen sich insbesondere deutsche Herstellerinnen schon seit längerem, um damit die höheren Preise ihrer Produkte zu rechtfertigen.

Wirtschaftsförderungsmaßnahme ohne Realweltkonsequenzen

Solange mangelhafte Konkurrenzprodukte ihren Preisvorteil durch geringe Investition und Nachsorge im Bereich der IT-Sicherheit ungehindert ausspielen können, ist allerdings nicht mit einer effektiven und nachhaltigen Erhöhung der bundesdeutschen IT-Sicherheit zu rechnen.

Die Konsequenzen gehen dabei nicht immer nur zulasten von Kundinnen der unsichereren Produkte: In Botnetzen zusammengeschlossene IoT-Geräte werden in der Regel weniger gegen ihre Eigentümerinnen als vielmehr gegen unbeteiligte Dritte eingesetzt. Die reine Existenz eines unsicheren Produkts in ausreichender Menge kann so zu Bedrohung für die nationale und internationale IT-Sicherheit werden.

Vor diesem Hintergrund auf freiwillige Sicherheitskennzeichen zu setzen, lässt ähnlich durchschlagenden Erfolg erwarten, wie bei der Eindämmung einer Pandemie auf Eigenverantwortung der Bürgerinnen zu hoffen: Es wäre wirklich zu schön, scheitert aber an der Realität.

Fehlende Überprüfung

Herstellerinnen sollen ihre Produkte durch Selbstzertifizierung ohne unabhängige Prüfung mit dem IT-Sicherheitskennzeichen des BSI schmücken dürfen. Dafür werden laut Gesetzentwurf für den Aufwand des BSI veranschlagt:

> *25 zusätzliche Planstellen/Stellen (17 hD; 8 gD) mit Personalkosten in Höhe von jährlich 2,33 Mio. Euro sowie Sacheinzelkosten in Höhe von 0,62 Mio. Euro jährlich.*

Empfehlung: Die 25 Planstellen sollten stattdessen einer zielgerichteten Aufgabe zugeführt werden, die auf eine tatsächliche Erhöhung der IT-Sicherheit ausgerichtet ist und so den Angestellten inhaltliche Erfüllung und eine berufliche Perspektive bieten kann.

Alternativen

Der CCC empfiehlt bei jeder sich bietenden Gelegenheit die Einführung einer Produkthaftung im Bereich der IT-Sicherheit zur Aktivierung der Selbstheilungskräfte der Herstellerinnen untauglicher Produkte sowie einen Update-Zwang bzw. ein "Mindesthaltbarkeitsdatum" als Markteintrittsvoraussetzung.[5152]

Haftung

In vielen Bereichen des Verbraucherschutzes hat sich die Produkthaftung als erfolgreiches Mittel erwiesen, Herstellerinnen zu einer effizienten und zielgerichteten Qualitätssicherung zu motivieren.

Eine entsprechende Haftung für Software-Produkte und Ansätze, auch für Open-Source-Software eine sinnvolle Lösung zu finden, hat der CCC bereit in einer früheren Stellungnahme erörtert[53] und zuletzt in einer Stellungnahme zum *Gesetzentwurf zur Umsetzung der Richtlinie über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte und digitaler Dienstleistungen Entwürfe zur Umsetzung der Richtlinie über digitale Inhalte und zu den vertraglichen Regelungen der Modernisierungsrichtlinie* eingebracht.[54]

Empfehlung: Der Chaos Computer Club rät zur Ausweitung der Produkthaftung auf den Bereich der IT-Sicherheit. Die Haftung sollte dann greifen, wenn die Herstellerin innerhalb eines angemessenen Zeitraums keine Abhilfe für bekannte IT-Sicherheitsmängel ihres Produkts geleistet hat.

---

[51] ccc.de: Stellungnahme des CCC zu Fragen der IT-Sicherheit in der Post-Snowden-Ära

[52] ccc.de: Update nicht verfügbar: Lieferant nicht zu erreichen

[53] ccc.de: Stellungnahme des CCC zu Fragen der IT-Sicherheit in der Post-Snowden-Ära

[54] bmjv.de: Chaos Computer Club: Anmerkungen und Ergänzungen zum Entwurf zur Umsetzung der Richtlinie über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte und digitaler Dienstleistungen, abgerufen am 26. Februar 2021

Updatezwang bzw. Mindesthaltbarkeitsdatum

Da IT-Sicherheit kein Zustand, sondern ein Prozess ist, kann diese durch Herstellerinnen nur glaubhaft und nachhaltig gewährleistet werden, wenn eine entsprechende Nachsorge betrieben wird: Wird ein Produkt oder eine Software-Lösung von der Herstellerin nicht mehr mit Updates versehen, wird die weitere Verwendung zum potenziell fahrlässigen Risiko.

Auch technisch einwandfreie Produkte können auf diese Weise zu teurem Elektroschrott oder Risiken für die nationale Sicherheit werden. Es ist daher unersichtlich, dass das Einsparen der unverzichtbaren Produktnachsorge weiterhin zum Marktvorteil gereicht.

Empfehlung: Der Chaos Computer Club rät zur Einführung eines "Mindesthaltbarkeitsdatums" hinsichtlich der IT-Sicherheit von Software und Geräten. Bis zum Ablauf des Mindesthaltbarkeitsdatums muss die Herstellerin verpflichtet sein, Sicherheitsupdates für das entsprechende Produkt bereitzustellen. Stellt die Herstellerin den Geschäftsbetrieb ein, oder die Nachsorge für ein Produkt vor Ablauf des Mindesthaltbarkeitsdatums ab, muss sie zur öffentlichen Bereitstellung des Quellcodes verpflichtet sein, um unabhängige Nachsorge zu ermöglichen.

Falscher Fokus auf "Unternehmen im besonderen öffentlichen Interesse"

Mit dem vorliegenden Gesetzentwurf soll das BSI auch Zuständigkeit für Unternehmen in besonderem öffentlichem Interesse erhalten. Als diese sollen Unternehmen gelten, die nicht unter die kritischen Infrastrukturen fallen, jedoch

a) Güter im Bereich der Kriegswaffen oder Produkte mit IT-Sicherheitsfunktionen zur Verarbeitung von staatlichen Verschlusssachen herstellen,

b) nach ihrer inländischen Wertschöpfung zu den größten Unternehmen in Deutschland gehören, oder

c) Gefahrenstoffe in großen Mengen an ihren Betriebsstätten vorhalten.

Während die Kriterien a) und c) grundsätzlich zumindest nachvollziehbar sind, erscheinen die Ressourcen des BSI bei den größten Unternehmen Deutschlands fehlinvestiert: Mängel und Unvermögen im Bereich der IT-Sicherheit sind vor allem in

kleineren Unternehmen prävalent, denen die Ressourcen und Verantwortlichkeiten für eine zeitgemäße IT-Sicherheit fehlen.

Während große Unternehmen individuelle, fähige und reife IT-Sicherheitsinfrastrukturen zu unterhalten in der Lage sind oder sein sollten, bleiben die gebetsmühlenartig gelobten “Hidden Champions”, die den deutschen Mittelstand und das Herz der deutschen Wirtschaft ausmachen sollen, vom Gesetzentwurf weiterhin unbeachtet.

Für kleine und mittelständische Unternehmen (KMU) hält der Gesetzentwurf die IT-Sicherheitskennzeichen bereit, die Herstellerinnen sich ohne unabhängige Prüfung selbst ausstellen können. Hier ist kein nennenswerter Effekt zu erwarten. Das ist tragisch, weil sich insbesondere bei den vielen KMU die Verwundbarkeit der Deutschen Wirtschaft offenbart und potenziert.

Empfehlung: Der Bundestag möge prüfen, welche Unternehmen im besonderen öffentlichen Interesse der Bundesrepublik liegen und welche davon tatsächlich besondere Aufmerksamkeit des BSI benötigen.

Empfehlung: Zum Schutz der KMU rät der CCC zur Förderung und Bereitstellung einer auf kompromisslose IT-Sicherheit ausgelegten Infrastruktur, zur Einführung einer Produkthaftung sowie zur Einführung eines Mindesthaltbarkeitsdatums.

Abschließende Bemerkungen

Der vorliegende Gesetzentwurf wird seit über zwei Jahren in unterschiedlichsten Varianten – meist unter Ausschluss der Öffentlichkeit – diskutiert. Von einigen besonders schlechten Ideen früherer Entwürfe wurde in der Zwischenzeit Abstand genommen.

Die Bemühungen des BMI, eine öffentliche Diskussion und zivilgesellschaftliche Beteiligung zu verhindern, haben dabei insgesamt eine neue Qualität erreicht. Höhepunkt dieser Bemühungen war das Einräumen einer Frist von 28 Stunden zur Kommentierung eines um 16 Seiten erweiterten Referentinnenentwurfs für ein zweites IT-Sicherheitsgesetz.

Der Chaos Computer Club hat dieses Vorgehen öffentlich streng kritisiert[55] und gehört zu den Unterzeichnerinnen eines offenen Briefes,[56] in dem eine Vielzahl digitalpolitischer Organisationen *„Angemessene Fristen statt Scheinbeteiligung"* fordert.

Unerlässlich sind hierbei:

1. Angemessene Fristen für die Kommentierung von Gesetzesentwürfen,
2. Bereitstellung von Synopsen zur besseren Vergleich- und Nachvollziehbarkeit,
3. Veröffentlichung der Referentenentwürfe auf den Webseiten der Ministerien und
4. eine Öffnung des Partizipationsprozesses

Empfehlung: Um ein drittes *Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme* in angemessener Qualität vorschlagen zu können, sollte das BMI seine Bemühungen zur aktiven Unterdrückung sachverständigen Rats einstellen.

[55] ccc.de: Innenministerium sabotiert sachkundige Diskussion zum IT-Sicherheitsgesetz 2.0

[56] ccc.de: Offener Brief an die Bundesregierung: Angemessene Fristen statt Scheinbeteiligung

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
19(4)512

Vorläufige Bewertung des Referentenentwurfs zum IT-Sicherheitsgesetz 2.0 vom 07.05.2020 und Empfehlungen

Autor:innen[1]

Dr. Sven Herpig, Leiter Internationale Cybersicherheitspolitik bei der Stiftung Neue Verantwortung

und

Jan-Peter Kleinhans, Leiter Technologie & Geopolitik bei der Stiftung Neue Verantwortung

Bereich 5G-Sicherheit/ Vertrauenswürdigkeitserklärung für Hersteller kritischer Komponenten

Die folgende Bewertung befasst sich mit dem Referentenentwurf des Bundesministeriums des Innern, für Bau und Heimat zum Zweiten Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme in der Fassung vom 7. Mai 2020, veröffentlicht auf Netzpolitik.org[2]*.*

[1] Ein Dank geht an die deutsche Cybersicherheitspolitik-Community für die Unterstützung bei der Erstellung dieser Bewertung.
[2] Andre Meister: Seehofer will BSI zur Hackerbehörde ausbauen

A. Gesamtkritik

Im Vergleich zum Referentenentwurf vom 27. März 2019[3] ist bei der vorliegenden Fassung vom 7. Mai 2020 zu begrüßen, dass die Änderungen zum StGB und StPO – und hier im Besonderen § 126a StGB, § 202e StGB, § 202f StGB und § 163g StPO - wie in der vorläufigen Bewertung vom 8. Mai 2019 angeregt[4], ersatzlos gestrichen worden sind. Nach gesicherten rechtswissenschaftlichen Erkenntnissen ist eine Verschärfung des Strafrechts kein geeignetes bzw. effektives Mittel zur Reduktion von Straftaten[5] und hätte in diesem Kontext daher auch nicht zu mehr IT-Sicherheit beigetragen.

Vor der Analyse spezifischer Einzelpunkte des Gesetzesentwurfs wird übergeordnet angeregt, dass sich der Bundestag in seiner Befassung allen Normen des vorliegenden Gesetzestextes widmet und nicht ausschließlich der Vertrauenswürdigkeitserklärung für Hersteller kritischer Komponenten u. a. § 9b BSIG-E („5G-Debatte“).

Diese Analyse des Gesetzesentwurfs mit angeschlossenen Empfehlungen befasst sich mit den folgenden Einzelpunkten:

1. IT-Sicherheit für die Gesellschaft durch Verbraucherschutz
2. Evaluierung der bisherigen IT- und Cybersicherheitsmaßnahmen
3. Mobile Incident Response Teams-Strategie
4. Unternehmen im besonderen öffentlichen Interesse
5. Schwachstellenmanagement und -meldewesen
6. Untersuchung der Sicherheit in der Informationstechnik
7. IT-Sicherheit in Digitalisierungsvorhaben
8. Kritische Komponenten und vertrauenswürdige Hersteller
9. Eingriff der Diensteanbieter in die Integrität von Kundensystemen
10. Anordnungsbefugnis gegenüber Kritischen Infrastrukturen und Infrastrukturen im besonderen öffentlichen Interesse
11. Pflichten der Diensteerbringer
12. Staatliche Cybersicherheitsarchitektur

Allgemein ist zu kritisieren, dass die Aktualisierung des Gesetzes ohne eine Evaluierung des vorangegangenen ersten IT-Sicherheitsgesetzes geplant wird, vor allem da ohne jegliche Evidenz von „Erfahrungen aus dem ersten IT-Sicherheitsgesetz“ (s. A. Allgemeiner Teil, II. Wesentlicher Inhalt des Entwurfs) gesprochen wird. Bereits bei dem Entwurf der Cybersicherheitsstrategie für Deutschland 2016 gab es keine Evaluierung der Cybersicherheitsstrategie 2011. Dieses Versäumnis wiegt in dem vorliegenden Vorhaben zum IT-Sicherheitsgesetz 2.0 noch weitaus schwerer, da im Vorgängergesetz sogar

[3] Andre Meister und Anna Biselli: T-Sicherheitsgesetz 2.0: Wir veröffentlichen den Entwurf, der das BSI zur Hackerbehörde machen soll
[4] Sven Herpig: Vorläufige Bewertung des Referentenentwurfs zum IT-Sicherheitsgesetz 2.0
[5] Siehe u. a. Wolfgang Heinz: Mehr und härtere Strafen = mehr Innere Sicherheit! Stimmt diese Gleichung? Strafrechtspolitik und Sanktionierungspraxis in Deutschland im Lichte kriminologischer Forschung

eine Teilevaluierung rechtlich verankert wurde.[6] Die Evaluierung von Maßnahmen ist ein elementarer Bestandteil staatlichen Handelns und sollte auch bei diesem Gesetzgebungsvorhaben durchgeführt werden, bevor eine Kompetenz- und Anforderungsausweitung verabschiedet wird. Der vorliegende Entwurf sieht zusätzlich weder eine Befristung noch eine gesonderte Evaluierung vor (Begründung, A. Allgemeiner Teil, VII. Befristung; Evaluierung). Stattdessen wird nur auf eine zukünftige gemeinsame Evaluierung beider IT-Sicherheitsgesetze ohne Spezifika verwiesen. Offensichtlich wird im Bereich der IT- und Cybersicherheitspolitik weiterhin versucht, sicherheitsbehördliche Kompetenzen auszubauen, ohne die Effektivität existierender Kompetenzen vorher zu evaluieren.
Der aktuelle Gesetzesentwurf ignoriert weiterhin die im Koalitionsvertrag[7] festgelegte "gleichzeitige und entsprechende Ausweitung der parlamentarischen Kontrolle" bei Ausweitung der Befugnisse der Sicherheitsbehörden. Das ist höchst problematisch, da die Bundesregierung bislang noch immer nicht die vom Bundesverfassungsgericht 2010 angeregte Gesamtschau der staatlichen Überwachungsmaßnahmen ("Überwachungsgesamtrechnung")[8] vorgelegt hat. Eine Befugnis-Erweiterung der Sicherheitsbehörden im IT-Sicherheitsgesetz 2.0 sollte unbedingt durch geeignete und angemessene Schutzmechanismen und Kontrollmaßnahmen begrenzt werden.

Auch auf die im Koalitionsvertrag vereinbarte Stärkung des Bundesamts für Sicherheit in der Informationstechnik "in seiner Rolle als unabhängige und neutrale Beratungsstelle für Fragen der IT-Sicherheit"[9] wird in dem Entwurf nicht eingegangen. Der Entwurf sollte zumindest eine Prüfung unterschiedlicher Unabhängigkeitsmodelle (z. B. Statistisches Bundesamt oder Bundesbeauftragter für den Datenschutz und die Informationsfreiheit)[10] vorsehen.

Zu dem Mangel empirischer Evidenz bei der Normengestaltung[11] und fehlender Berücksichtigung der Vorgaben aus dem Koalitionsvertrag kommen weitere Defizite, auf die im Folgenden eingegangen wird. Eine Überarbeitung des Referentenentwurfs wäre daher notwendig und zielführend, um die Cyber- und Informationssicherheit in Deutschland nachhaltig zu stärken.

[6] Bundesanzeiger: Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz)
[7] Bundesregierung: Koalitionsvertrag zwischen CDU, CSU und SPD
[8] digitalcourage: Überwachungsgesamtrechnung
[9] Bundesregierung: Koalitionsvertrag zwischen CDU, CSU und SPD
[10] Sven Herpig: Sachverständigenstellungnahme im Ausschuss des Deutschen Bundestags für Inneres und Heimat
[11] Sven Herpig: Sachverständigenstellungnahme im Ausschuss des Deutschen Bundestags für Inneres und Heimat

Stiftung Neue Verantwortung

B. Einzelkritik (nicht abschließend)

1. IT-Sicherheit für die Gesellschaft durch Verbraucherschutz

A. „Problem und Ziel“ in Verbindung mit „B. Lösung“ und Verweis auf §§ 3 und 9a BSIG-E

Der Entwurf definiert den Schutz von Gesellschaft als eines der Kernziele des Gesetzes. Als Hauptmaßnahme zum Schutz der Bürger:innen, und der damit verbundenen größten Personalaufwendung, führt der Entwurf die Einführung des „IT-Sicherheitskennzeichens“ an. Allerdings wird das IT-Sicherheitskennzeichen nicht direkt zu einer Erhöhung der IT- und Cybersicherheit in Deutschland führen. Eine indirekte Erhöhung der IT- und Cybersicherheit wäre bei verpflichtenden IT-Sicherheitssiegeln zumindest durch die Beeinflussung der Kaufentscheidung und des damit einhergehenden Einflusses auf Hersteller, die sich um eine verbesserte IT-Sicherheit ihrer Produkte bemühen müssten, gegeben.[12] Wenn eine Kennzeichnung mit dem IT-Sicherheitskennzeichen in Verbindung mit dem elektronischen Beipackzettel freiwillig ist, signalisiert es nur, wie (un)sicher ein Produkt ist. Weder die Produkte noch die Bürger:innen/Gesellschaft werden damit direkt sicherer. Zugespitzt bedeutet dies, dass IT-Produkte, deren Schutzmechanismen im Entwurf selbst als „faktisch wirkungslos“ bezeichnet werden, weiterhin verkauft werden dürften und nur auf Basis von Freiwilligkeit des Herstellers ein entsprechendes IT-(Un)Sicherheitskennzeichen auf der Verpackung tragen würden. Gleichzeitig entsteht durch die in §§ 9a und 3 Absatz 14 BSIG-E erwähnten Aufgaben ein hoher Mehraufwand für das Bundesamt für Sicherheit in der Informationstechnik. Es ist zu bezweifeln, dass der Ertrag den Aufwand beim freiwilligen IT-Sicherheitskennzeichen rechtfertigt. Die Maßnahme ist möglicherweise effektiv, aber keineswegs effizient. Vor dem Hintergrund der nach wie vor herrschenden Knappheit an IT-Sicherheitsfachkräften im öffentlichen Dienst sollte diese Maßnahme dringend überdacht werden.

Empfehlung: Die Bundesregierung sollte darauf hinarbeiten, dass bekanntermaßen unsichere und nicht mehr absicherbare IT-Produkte überhaupt nicht in den Handel gelangen dürfen.[13] Weiterhin sollten konkrete Maßnahmen ergriffen werden, die direkt für eine höhere Sicherheit der Bürger:innen sorgen, wie z. B. eine voreingestellte Netzwerksegmentierung bei Routern (Heimnetz/ IoT-Geräte). Die Idee des IT-Sicherheitskennzeichens sollte stattdessen direkt auf EU-Ebene angegangen werden, damit der Einsatz von verpflichtenden statt nur freiwilligen Siegeln ermöglicht werden kann (siehe „Warenverkehrsfreiheit“). Gleichzeitig muss sichergestellt werden, dass ein (freiwilliges) IT-Sicherheitskennzeichen nicht mit höherwertigen Zertifizierungen von Produkten vermischt wird.

[12] Philipp Morgner, Christoph Mai, Nicole Koschate-Fischer, Felix Freiling und Zinaida Benenson: Security Update Labels: Establishing Economic Incentives for Security Patching of IoT Consumer Products
[13] Verbraucherzentrale Nordrhein-Westfalen: Vorerst keine Sicherheit für Handynutzer: Urteil Oberlandesgericht Köln

2. Evaluierung der bisherigen IT- und Cybersicherheitsmaßnahmen

„A. Problem und Ziel“ in Verbindung mit „C. Alternativen“

Als sehr weit gefasste Zielvorgabe gibt der Entwurf vor, dass das Gesetz „dem Schutz von Staat, Wirtschaft und Gesellschaft“ dienen soll. Eine Alternative zu allen im Entwurf vorgeschlagenen Normen wird nicht genannt. Es ist schwer nachvollziehbar, dass bei einer so umfassenden Zielvorgabe keine einzige Alternative genannt werden kann. Dies ist möglicherweise auf die fehlende Evaluierung der Effektivität der bisher implementierten staatlichen Maßnahmen zur Erhöhung der Cyber- und IT-Sicherheit in Deutschland zurückzuführen.

Empfehlung: Die Bundesregierung sollte die Effektivität der bisher getroffen Cyber- und IT-Sicherheitsmaßnahmen evaluieren und unter Einbeziehung der Expertise aus Wirtschaft, Wissenschaft und Zivilgesellschaft Alternativen entwerfen, bevor der vorliegende Gesetzestext als alternativlos bezeichnet wird.

3. Mobile Incident Response Teams-Strategie

„E.3 Erfüllungsaufwand der Verwaltung“ in Verbindung mit § 5a BSIG-E

Die Mobile Incident Response Teams (MIRTs) des Bundesamtes für Sicherheit in der Informationstechnik sind ein Kernelement reaktiver Maßnahmen in der deutschen Cyber- und IT-Sicherheitspolitik. Der Mehrwert der MIRTs für die deutsche Cyber- und IT-Sicherheitspolitik ist für die Öffentlichkeit nachvollziehbar, wie u. a. der Fall des Lukaskrankenhauses in Neuss[14] gezeigt hat.

Empfehlung: Ein Ausbau der MIRTs ist zu unterstützen, da für diese eine breite Fachexpertise – zum Beispiel für die unterschiedlichen Systeme Kritischer Infrastrukturen – bereitgehalten werden muss. Der genannte Ausbau der Teams wäre eine effiziente Investition der im Entwurf insgesamt vorgesehenen Personalressourcen. Es ist dabei jedoch unklar, wie viele MIRTs notwendig sind, u. a. wegen Bereitschaftszeiten und Spezialexpertise. Es sollte daher dargelegt werden, welcher Plan hinter dem Ausbau der MIRTs steht und wie viele dieser Teams zu welchem Zeitpunkt für welche Einsatzgebiete (Regierung, KRITIS o. ä.) bereitstehen müssen. Dieser Plan sollte auch Transparenz über Einsatzstatus, Aufgabenteilung und Einsatzgebiete der „Quick Reaction Forces“ des Bundeskriminalamts, der „Mobile Cyber-Teams“ des Bundesamts für Verfassungsschutz und analoger Teams des Militärischen Abschirmdiensts und Bundesnachrichtendiensts herstellen.[15] Zudem sollte eine Einbettung des Konzepts des Cyber-Hilfswerks[16] in diesen Plan geprüft werden. Eine Integration des Mobile Incident Response Team Plans in den „Gesamtplan für die Reaktionsmaßnahmen des Bundes“ gem. § 5c BSIG-E wäre zielführend.

[14] Noah Gottschalk: Wenn eine Klinik ohne Computer arbeiten muss
[15] Bundesministerium des Innern: Cyber-Sicherheitsstrategie für Deutschland 2015
[16] AG KRITIS: Cyber-Hilfswerk (CHW)

4. Unternehmen im besonderen öffentlichen Interesse

§ 2 Absatz 14 BSIG-E in Verbindung mit §§ 8f und 10 Absatz 5 BSIG-E

Es ist unklar, in welchem Verhältnis die im Gesetz genannten „Institutionen im besonderen staatlichen Interesse" (INSI)[17] zu den im Entwurf erstmals erwähnten „Unternehmen im besonderen öffentlichen Interesse" gem. § 8f BSIG-E und der „Infrastruktur im besonderen öffentlichen Interesse“ gem. § 109a Abs 8 TKG-E stehen. Weder in der EU NIS-Richtlinie[18] noch in dem entsprechenden Umsetzungsgesetz[19] finden sich diese Begrifflichkeiten wieder. Im Umsetzungsgesetz wird lediglich einmal von „informationstechnischen Systemen von besonderem öffentlichem Interesse" gesprochen (§ 5a Absatz 2 BSIG). Diese Inkonsistenzen wirken einer Harmonisierung entgegen und verstärken die Komplexität durch die unilaterale Einführung einer weiteren „Schutzklasse“. Weiterhin ist nicht ersichtlich, warum politische Parteien von der KRITIS-Regulierung und der Regulierung für die „Unternehmen im besonderen öffentlichen Interesse“ ausgenommen sein sollten. Parteien sind Kernelemente des politischen Systems, und damit kritisch für die Demokratie in Deutschland. Sie sollten als solche daher entsprechend hohe IT-Sicherheitsstandards erfüllen.[20]

Empfehlung: Die Bundesregierung muss Transparenz bzgl. der „Institutionen im besonderen staatlichen Interesse“ im Vergleich zu „Unternehmen im besonderen öffentlichen Interesse“ und „Infrastruktur im besonderen öffentlichen Interesse“ schaffen. Gleichzeitig sollten die Kategorien der deutschen Gesetzgebung nicht von der EU-Harmonisierung abweichen, weshalb eine zusätzliche, unilaterale Einführung der „Unternehmen im besonderen öffentlichen Interesse“ o. ä. verworfen werden sollte. Auch inhaltlich erscheint diese zusätzliche Kategorie nicht sinnvoll: Entweder werden Unternehmen als kritisch genug betrachtet, um sie bzgl. IT-Sicherheit zu regulieren und folglich unter der KRITIS-Regulierung zu subsumieren, oder aber sie werden als nicht relevant genug eingeordnet, um bzgl. IT-Sicherheit reguliert zu werden. In diesem Fall können sie dann unter den bestehenden, unbestimmten Rechtsbegriff der „Institutionen im besonderen staatlichen Interesse“ fallen. Eine Ausdifferenzierung kann bei Aufnahme in die KRITIS-Regulierung über die branchenspezifischen Sicherheitsstandards[21] stattfinden. Darüber hinaus ist zu prüfen, ob politische Parteien wegen ihrer Relevanz für das Funktionieren des deutschen Staates in die KRITIS-Regulierung aufgenommen werden sollten. Sollte die Bundesregierung an der Einführung der zusätzlichen Kategorie „Unternehmen im besonderen öffentlichen Interesse“ festhalten, so ist zumindest § 10 Absatz 5 BSIG-E um die Beteiligung der organisierten Zivilgesellschaft zu erweitern.

[17] Bundesamt für Sicherheit in der Informationstechnik: Aktiv für mehr Cyber-Sicherheit
[18] Amtsblatt der Europäischen Union: RICHTLINIE (EU) 2016/1148 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 6. Juli 2016
[19] Bundesgesetzblatt: Gesetz zur Umsetzung der Richtlinie (EU) 2016/1148des Europäischen Parlaments und des Rates vom 6. Juli 2016
[20] Sven Herpig und Julia Schuetze: Mehr IT-Sicherheit für deutsche Wahlen
[21] Bundesamt für Sicherheit in der Informationstechnik: Branchenspezifische Sicherheitsstandards

5. Schwachstellenmanagement und -meldewesen

§ 4b BSIG-E in Verbindung mit §§ 7, 7a, 7b und 7c BSIG-E

Der Umgang mit Schwachstellen ist einer der wichtigsten Aspekte zur Herstellung von IT-Sicherheit in Unternehmen und Behörden. Klare Prozesse und Verantwortlichkeiten, die der technischen Komplexität Rechnung tragen, sind daher unbedingt notwendig. Die mit dem Entwurf geplante Regulierung bzgl. des staatlichen Schwachstellenmanagements und -meldewesens ist vollkommen intransparent. Es ist zu erwarten, dass diese Intransparenz zu ineffektiven Prozessen und einem Vertrauensverlust bei Firmen und IT-Sicherheitsforscher:innen -- Akteuren, die elementar für eine solche Policy sind -- führen wird.

Empfehlung: Empfohlen wird ein Verweis auf eine separate Verordnung o. ä., die den Umgang mit Schwachstellen durch Behörden dezidiert regelt, anstatt einer Regelung der Prozesse über die im Entwurf angeführten Normen. Zudem wird eine Einführung des seit Jahren in Planung befindlichen Schwachstellenmanagements des Bundesministeriums des Innern, für Bau und Heimat am Beispiel des von der Stiftung Neue Verantwortung vorgelegten Entwurfs empfohlen[22]. Gleichzeitig sollte ein Errichtungsgesetz für die Schwachstellen-verarbeitende Zentrale Stelle für Sicherheit in der Informationstechnik erarbeitet werden. Das ist dringend notwendig, da die Behörde ihre invasive Tätigkeit momentan ohne eine solche Gesetzesgrundlage ausübt. In den Gesetzen aller Schwachstellen-verarbeitenden Sicherheitsbehörden auf Bundesebene (u. a. Bundesnachrichtendienst, Bundeskriminalamt, Bundespolizei, Bundesamt für Verfassungsschutz, Bundeswehr, Zentrale Stelle für Sicherheit in der Informationstechnik) muss eine Reziprozität bzgl. der Weitergabe von Schwachstellen ergänzt werden: Während das Bundesamt für Sicherheit in der Informationstechnik gem. § 3 Absatz 1 Satz 13 BSIG andere Bundesbehörden bei der Wahrnehmung ihrer gesetzlichen Aufgaben unterstützen muss, sind diese Bundesbehörden ihrerseits nicht verpflichtet, das Bundesamt für Sicherheit in der Informationstechnik durch die Weitergabe der von ihnen gefundenen oder erworbenen Schwachstellen zu unterstützen. Dies ist allerdings eine Grundvoraussetzung für die Wahrnehmung der gesetzlichen Aufgaben des Bundesamtes für Sicherheit in der Informationstechnik.

Auch vor diesem Hintergrund wäre eine stärkere fachliche Unabhängigkeit des Bundesamtes für Sicherheit in der Informationstechnik vom Bundesministerium des Innern, für Bau und Heimat zielführend.

[22] Sven Herpig: Schwachstellen-Management für mehr Sicherheit

6. Untersuchung der Sicherheit in der Informationstechnik

§ 7a BSIG-E in Verbindung mit §§ 7, 7a, 7b und 7c BSIG-E

Die Norm enthält keinerlei Einschränkung darüber, welche informationstechnischen Produkte und Systeme das Bundesamt für Sicherheit in der Informationstechnik untersuchen darf (Absatz 1). Darüber hinaus darf das Bundesamt für Sicherheit in der Informationstechnik in diesem Kontext alle notwendigen Informationen von den Herstellern einfordern (Absatz 2). Eine anlasslose Untersuchung aller informationstechnischen Produkte und Systeme mit einer zusätzlichen Befugnis, externe Informationen anzufordern, ist sehr breit. Gleichzeitig werden dem Bundesamt kaum Beschränkungen auferlegt, wie es mit den so erworbenen Informationen verfahren darf (Verweis auf die sehr breite Norm § 3 Absatz 1 Satz 2 BSIG). Dies könnte folglich auch die Weitergabe von Informationen zu Schwachstellen an andere Sicherheitsbehörden beinhalten, welche die Schwachstellen ausnutzen und damit dem gesetzlichen Auftrag des Bundesamtes für Sicherheit in der Informationstechnik zuwiderhandeln würden.

Empfehlung: Zusätzlich zu den unter „5. Schwachstellenmanagement und -meldewesen“ genannten Empfehlungen sollte aufgrund der vorausgegangenen Analyse zumindest eine defensive Zweckbindung der so erlangten Informationen über die IT-Produkte und Systeme eingefügt werden (Absätze 2 und 3). Zusätzlich sollte eine Verengung der Norm geprüft werden.

7. IT-Sicherheit in Digitalisierungsvorhaben

§ 8 Absatz 4 BSIG-E

Die Zeitangabe “frühzeitig” im Kontext der Einbindung des Bundesamtes für Sicherheit in der Informationstechnik in Digitalisierungsvorhaben des Bundes wird in dieser Norm nicht näher definiert. Zusätzlich ist das Bundesamt für Sicherheit in der Informationstechnik gegenüber dem Bundesministerium des Innern, für Bau und Heimat fachlich weisungsgebunden und das Ministerium muss über jede Zusammenarbeit des Bundesamts für Sicherheit in der Informationstechnik informiert werden (vgl. § 26 GGO). Vor dem Hintergrund dieser Beschränkungen führt die Norm wahrscheinlich nicht zu der beabsichtigten früheren Einbindung des Bundesamts für Sicherheit in der Informationstechnik in Digitalisierungsvorhaben der Bundesverwaltung.

Empfehlung: Die Angabe „frühzeitig“ sollte präzisiert bzw. ein grober Zeitraum inkludiert werden. Weiterhin sollte ermöglicht werden, dass andere Behörden die Unterstützung des Bundesamts für Sicherheit in der Informationstechnik direkt und ohne vorherigen Kontakt zum Bundesministerium des Innern, für Bau und Heimat ersuchen können. Das würde auch die im Koalitionsvertrag angekündigte Stärkung des Bundesamts für Sicherheit in der Informationstechnik "in seiner Rolle als unabhängige und neutrale Beratungsstelle für Fragen der IT-Sicherheit"[23] fördern.

[23] Bundesregierung: Koalitionsvertrag zwischen CDU, CSU und SPD

8. Kritische Komponenten und vertrauenswürdige Hersteller

§ 9b BSIG-E in Verbindung mit § 2 Absatz 13 BSIG-E

Die sehr breite Definition von „kritischen Komponenten“ in Verbindung mit der Garantieerklärung über die „gesamte Lieferkette des Herstellers“ auf Basis einer nicht näher definierten späteren Allgemeinverfügung des Bundesministeriums des Innern, für Bau und Heimat macht eine Bewertung dieser Norm ohne weitere Details schwer möglich. Der Anwendungsbereich dieser Norm geht weit über die technische IT- und Cybersicherheit hinaus, für die das Bundesamt für Sicherheit in der Informationstechnik – und damit das BSIG – verantwortlich ist. Dies wird unter anderem dadurch deutlich, dass in diesem Kontext das Bundesministerium des Innern, für Bau und Heimat und nicht mehr das Bundesamt für Sicherheit in der Informationstechnik genannt wird. Diese Perspektive wird u. a. dadurch verstärkt, dass der Text nicht mehr auf die „Grundwerte der Informationssicherheit“ (Verfügbarkeit, Vertraulichkeit und Integrität)[24] verweist, sondern „Vertraulichkeit“ weglässt und stattdessen die Kategorien „Funktionsfähigkeit“ und „Sicherheit“ anführt. Es handelt sich hierbei um außen- und sicherheitspolitische Normen, die nicht über das BSIG geklärt werden sollten.

In der Begründung zu § 9b BSIG-E wird zu Recht festgestellt, dass die Zertifizierung der IT-Sicherheit einer kritischen Komponente nicht die Überprüfung der Vertrauenswürdigkeit eines Herstellers umfasst und beides zwingend getrennt betrachtet werden muss. Die aufgelisteten Kriterien (§ 9b Absatz 4 BSIG-E) zur Einschätzung der Vertrauenswürdigkeit eines Herstellers adressieren jedoch ausschließlich technische Risiken (Penetrationstests, Schwachstellen-Management, “Hintertüren”). Eine ganzheitliche Einschätzung der Vertrauenswürdigkeit eines Herstellers wird dadurch verfehlt.

Weiterhin besagt § 9b Absatz 4 Punkt 5 BSIG-E, dass ein Hersteller nicht vertrauenswürdig sei, wenn „die kritische Komponente über technische Eigenschaften verfügt, die geeignet sind, missbräuchlich auf die Sicherheit, Integrität, Verfügbarkeit oder Funktionsfähigkeit der Kritischen Infrastruktur einwirken zu können.” Dieses Kriterium ist nicht geeignet, um die Vertrauenswürdigkeit eines Herstellers einzuschätzen, da Netzwerkkomponenten immer eine solche Fernwartungsschnittstelle besitzen, über die die Netzwerkkomponente kontrolliert werden kann. Eine solche Schnittstelle kann in jedem Fall durch Betreiber und unter Umständen auch durch den Komponentenhersteller benutzt werden, um „missbräuchlich auf die Sicherheit, Integrität, Verfügbarkeit oder Funktionsfähigkeit der Kritischen Infrastruktur” einzuwirken. Das Verbot eines solchen Fernwartungszugangs ist nicht möglich. Damit bleibt das Kriterium wirkungslos.[25] Die Vertrauenswürdigkeit eines Herstellers muss, unabhängig von der IT-Sicherheitszertifizierung der Komponenten, anhand von nicht-technischen Kriterien überprüft werden. Eine solche Überprüfung kann nicht durch das Bundesamt für Sicherheit in der Informationstechnik geleistet werden, sondern muss zwingend durch mehrere Ressorts erfolgen. Die Grundlage hierfür sollte daher nicht im BSIG-E gelegt werden.

Empfehlung: Die Norm § 9b BSIG-E sollte ersatzlos gestrichen und in ein separates Gesetzesvorhaben überführt werden.

[24] Bundesamt für Sicherheit in der Informationstechnik: IT-Grundschutz Glossar
[25] Jan-Peter Kleinhans: Whom to trust in a 5G world?

9. Eingriff der Diensteanbieter in die Integrität von Kundensystemen

§ 109a Absatz 8 TKG-E in Verbindung mit § 109a Absätze 4,5 und 6 sowie § 149 Absatz 1 TKG

Es handelt sich hierbei um einen angeordneten Eingriff in das Computergrundrecht[26]. Es ist unklar, wie die operative Umsetzung aussähe und welche Schutzmechanismen ergriffen würden, um die Verfügbarkeit und Vertraulichkeit der betroffenen Datenverarbeitungssysteme durch die Veränderung der Integrität nicht zu beeinträchtigen. Darüber hinaus leistet Absatz 8 im Sinne der IT- und Cybersicherheit keinen erkennbaren zusätzlichen Schutz zu den Maßnahmen gem. der Absätze 4, 5 und 6. Eine Nichteinhaltung ist mit Bußgeldforderungen belegt.

Empfehlung: § 109a Absatz 8 TKG-E sollte ersatzlos gestrichen werden.

10. Anordnungsbefugnis gegenüber Diensteanbietern

§ 13 Absatz 7a TMG-E

In dieser sehr weit und unpräzise gefassten Norm (Beispiel: „Vielzahl von Nutzern“) bleibt die Haftungsfrage bei Nutzung der neu geschaffenen Anordnungsbefugnis ungeklärt. Dies ist vor dem Hintergrund eines möglicherweise sehr hohen Erfüllungsaufwands - vgl. Reichweite der Norm in Verbindung mit der Eingriffstiefe - für Dritte sehr problematisch.

Empfehlung: Eine Klärung der Haftungsfrage – vor allem vor dem Hintergrund der Eingriffstiefe der Anordnungen – sowie die klare Abgrenzung der unterschiedlichen Kategorien voneinander scheinen zwingend notwendig. Weiterhin muss geklärt werden, wie weit die Anordnungsbefugnis reicht (u. a. bis zur Produktentwicklung). Entsprechend des Umfangs der Norm muss dem Erfüllungsaufwand Dritter mit adäquaten Haftungsregelungen oder Ausgleichsmaßnahmen entgegengewirkt werden.

11. Pflichten der Diensteerbringer

§ 15b Abs 1 TMG-E

Es handelt sich hierbei um eine zu weitgefasste Norm, die unter anderem auf einer unklaren Begründung des Staatswohls – vgl. § 15b Abs 1 Satz 3 TMG-E – basiert. Problematisch ist weiterhin, dass keine Bereichsausnahmen für Tätigkeiten im öffentlichen Interesse, zum Beispiel für die Arbeit der Presse, vorgesehen sind. Es ist anzuzweifeln, dass Diensteerbringer in der Vergangenheit einer entsprechenden Verpflichtung gem. § 15b Abs 1 TMG-E wissentlich nicht gefolgt sind. Weiterhin stellt § 15b Abs 2 TMG-E ohne Anordnung durch zuständige Behörden, zum Beispiel durch das Bundeskriminalamt, einen möglicherweise unverhältnismäßigen Aufwand für die Diensteerbringer dar.

Empfehlung: Es ist zu prüfen, ob eine empirische Grundlage für § 15b Abs 1 TMG-E gewährleistet ist, gemäß derer Diensteerbringer dieser Pflicht nicht nachgekommen sind. § 15b Abs 2 TMG-E sollte

[26] Bundesverfassungsgericht: Leitsätze zum Urteil des Ersten Senats vom 27. Februar 2008- 1 BvR 370/07 -- 1 BvR 595/07 -

ausschließlich eine zwingende und nicht optionale Anordnung der zuständigen Stellen vorsehen. Die Norm sollte um § 15b Abs 4 TMG-E ergänzt werden, der eine Ausnahme von den Absätzen 1-3 vorsieht, sobald die zur Veröffentlichung vorgesehenen Daten dem öffentlichen Interesse dienen. Dies sollte insbesondere dann gelten, wenn das Handeln im Einklang mit § 5 GeschGehG und dem geltenden Datenschutzrecht, sowie den hierin enthaltenen Bereichsausnahmen medialer Arbeit (beispielhaft: § 12 LPG NRW, § 59 RStV) steht.

12. Staatliche Cybersicherheitsarchitektur

„Begründung", „Allgemeiner Teil", „VI. Gesetzesfolgen", „2. Nachhaltigkeitsaspekte"

Im Referentenentwurf heißt es, dass der Inhalt des Entwurfs der „deutschen IT-Sicherheitsarchitektur" entspricht. Auf welche Grundlage sich dieser Terminus bezieht, bleibt dabei völlig unklar. Die einzig bisher bekannte Übersicht zur staatlichen Cybersicherheitsarchitektur in Deutschland wurde von der Stiftung Neue Verantwortung veröffentlicht.[27] Der Referentenentwurf verliert unabhängig davon kein Wort über eine notwendige Reform der offensichtlich dysfunktionalen, zentralen Akteure der deutschen Cybersicherheitsarchitektur, dem Cyber-Abwehrzentrum und dem Cyber-Sicherheitsrat.

Empfehlung: Das IT-Sicherheitsgesetz 2.0 sollte genutzt werden, um die Strukturen des Cyber-Abwehrzentrums und des Cyber-Sicherheitsrats zu klären und eine rechtliche Grundlage für die Arbeit dieser Institutionen, und der Zentralen Stelle für Informationstechnik im Sicherheitsbereich, zu schaffen. Dies sollte unter anderem Kooperationsmöglichkeiten und -grenzen, Verantwortlichkeiten, Aufgaben und Verortung in der deutschen Cybersicherheitsarchitektur beinhalten. Hierzu gehört beispielsweise die Trennung zwischen operativen und nicht operativen Aufgaben im Bereich der Cybersicherheit (vgl. u. a. BVerfG Leitsätze zum Urteil des Ersten Senats vom 19. Mai 2020)[28]. Weiterhin sollte die Bundesregierung einen Plan zu Weiterentwicklung der deutschen Cybersicherheitsarchitektur vorlegen, insbesondere vor dem Hintergrund der Gründung immer neuer Institutionen wie der Zentralen Stelle für Sicherheit in der Informationstechnik, der Agentur für Sprunginnovationen, der Cyberagentur, dem Zentrum für Digitalisierungs- und Technologieforschung der Bundeswehr und vielen mehr, und damit möglicherweise entstehender unklarer Verantwortlichkeiten und Parallelstrukturen entgegenwirken.

[27] Sven Herpig und Rebecca Beigel: Akteure und Zuständigkeiten in der deutschen Cybersicherheitspolitik
[28] Bundesverfassungsgericht: Leitsätze zum Urteil des Ersten Senats vom 19. Mai 2020 - 1 BvR 2835/17 – [5. Leitsatz]

Stiftung Neue Verantwortung

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
19(4)662 neu

Stellungnahme zum Referentenentwurf „IT-Sicherheitsgesetz 2.0“ – in der Fassung vom 01.12.2020[1] – des Bundesministeriums des Innern, für Bau und Heimat

Autor:innen[2]

Dr. Sven Herpig, Leiter Internationale Cybersicherheitspolitik bei der Stiftung Neue Verantwortung

und

Jan-Peter Kleinhans, Leiter Technologie & Geopolitik bei der Stiftung Neue Verantwortung

Bereich 5G-Sicherheit/ Vertrauenswürdigkeitserklärung für Hersteller kritischer Komponenten

[1] Bundesministerium des Innern, für Bau und Heimat (2020): Referentenentwurf des Bundesministeriums des Innern, für Bau und Heimat Entwurf eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme

[2] Ein Dank geht an die deutsche Cybersicherheitspolitik-Community für die Unterstützung bei der Analyse.

Stiftung Neue Verantwortung

A. Gesamtkritik

Im Vergleich zum Referentenentwurf vom 27. März 2019[3] ist bei der vorliegenden Fassung vom 7. Mai 2020 zu begrüßen, dass die Änderungen zum StGB und StPO – und hier im Besonderen § 126a StGB, § 202e StGB, § 202f StGB und § 163g StPO - wie in der vorläufigen Bewertung vom 8. Mai 2019 angeregt[4], ersatzlos gestrichen worden sind. Nach gesicherten rechtswissenschaftlichen Erkenntnissen ist eine Verschärfung des Strafrechts kein geeignetes bzw. effektives Mittel zur Reduktion von Straftaten[5] und hätte in diesem Kontext daher auch nicht zu mehr IT-Sicherheit beigetragen.

Im Vergleich zum Referentenentwurf vom 7. Mai 2020[6] ist bei der vorliegenden Fassung vom 1. Dezember zu begrüßen, dass durch Auslassung des Begriffs „Infrastruktur im besonderen öffentlichen Interesse" mehr Klarheit bei der Terminologie geschaffen wurde (vgl. *4. Unternehmen im besonderen öffentlichen Interesse*), wie in der vorläufigen Bewertung vom 9. Juni 2020 angeregt. Weiterhin ist zu begrüßen, dass – wie auch in der vorläufigen Bewertung angeregt – die Norm § 7a BSIG-E Absatz 1 Satz 2 auf Nummern 1, 14, 14a, 17 und 18 verengt wurde (vgl. *6. Untersuchung der Sicherheit in der Informationstechnik*).

Vor der Analyse spezifischer Einzelpunkte des Gesetzesentwurfs wird übergeordnet angeregt, dass sich der Bundestag in seiner Befassung allen Normen des vorliegenden Gesetzestextes widmet und nicht ausschließlich der Vertrauenswürdigkeitserklärung für Hersteller kritischer Komponenten u. a. § 9b BSIG-E („5G-Debatte").

Diese Analyse des Gesetzesentwurfs mit angeschlossenen Empfehlungen befasst sich mit den folgenden Einzelpunkten:

1. IT-Sicherheit für die Gesellschaft durch Verbraucherschutz
2. Evaluierung der bisherigen IT- und Cybersicherheitsmaßnahmen
3. Mobile Incident Response Teams
4. Unternehmen im besonderen öffentlichen Interesse und Parteien
5. Schwachstellenmanagement und -meldewesen
6. Untersuchung der Sicherheit in der Informationstechnik
7. IT-Sicherheit in Digitalisierungsvorhaben
8. Kritische Komponenten und vertrauenswürdige Hersteller
9. Eingriff der Diensteanbieter in die Integrität von Kundensystemen
10. Anordnungsbefugnis gegenüber Diensteanbietern
11. Pflichten der Diensteerbringer
12. Sonderrolle von Auswärtigem Amt und Bundeswehr
13. Staatliche Cybersicherheitsarchitektur

[3] Andre Meister und Anna Biselli: T-Sicherheitsgesetz 2.0: Wir veröffentlichen den Entwurf, der das BSI zur Hackerbehörde machen soll
[4] Sven Herpig: Vorläufige Bewertung des Referentenentwurfs zum IT-Sicherheitsgesetz 2.0
[5] Siehe u. a. Wolfgang Heinz: Mehr und härtere Strafen = mehr Innere Sicherheit! Stimmt diese Gleichung? Strafrechtspolitik und Sanktionierungspraxis in Deutschland im Lichte kriminologischer Forschung
[6] Andre Meister: Seehofer will BSI zur Hackerbehörde ausbauen

Allgemein ist zu kritisieren, dass die Aktualisierung des Gesetzes ohne eine Evaluierung des vorangegangenen ersten IT-Sicherheitsgesetzes geplant wird, vor allem da ohne jegliche Evidenz von „Erfahrungen mit der Anwendung der im ersten IT-Sicherheitsgesetz geregelten Befugnisse“ (s. A. Allgemeiner Teil, II. Wesentlicher Inhalt des Entwurfs) gesprochen wird. Bereits bei dem Entwurf der Cybersicherheitsstrategie für Deutschland 2016 gab es keine Evaluierung der Cybersicherheitsstrategie 2011. Dieses Versäumnis wiegt in dem vorliegenden Vorhaben zum IT-Sicherheitsgesetz 2.0 noch weitaus schwerer, da im Vorgängergesetz sogar eine Teilevaluierung rechtlich verankert wurde.[7] Die Evaluierung von Maßnahmen ist ein elementarer Bestandteil staatlichen Handelns und sollte auch bei diesem Gesetzgebungsvorhaben durchgeführt werden, bevor eine Kompetenz- und Anforderungsausweitung verabschiedet wird. Der vorliegende Entwurf sieht zusätzlich weder eine Befristung noch eine gesonderte Evaluierung vor (Begründung, A. Allgemeiner Teil, VII. Befristung; Evaluierung). Stattdessen wird unbestimmt „[d]ie in Artikel 10 IT-Sicherheitsgesetz vorgesehene Evaluierung […] mit diesem Gesetz auf einen Zeitpunkt verschoben, zu dem bereits eine ausreichende Erfahrungsgrundlage für eine Evaluierung besteht und zudem entsprechend der Neufassung des BSIG aktualisiert“ (Zu Artikel 6). Offensichtlich wird im Bereich der IT- und Cybersicherheitspolitik weiterhin versucht, sicherheitsbehördliche Kompetenzen auszubauen, ohne die Effektivität existierender Kompetenzen vorher zu evaluieren.
Der aktuelle Gesetzesentwurf ignoriert weiterhin die im Koalitionsvertrag[8] festgelegte "gleichzeitige und entsprechende Ausweitung der parlamentarischen Kontrolle" bei Ausweitung der Befugnisse der Sicherheitsbehörden. Das ist höchst problematisch, da die Bundesregierung bislang noch immer nicht die vom Bundesverfassungsgericht 2010 angeregte Gesamtschau der staatlichen Überwachungsmaßnahmen ("Überwachungsgesamtrechnung")[9] vorgelegt hat. Eine Befugnis-Erweiterung der Sicherheitsbehörden im IT-Sicherheitsgesetz 2.0 sollte unbedingt durch geeignete und angemessene Schutzmechanismen und Kontrollmaßnahmen begrenzt werden.

Auch auf die im Koalitionsvertrag vereinbarte Stärkung des Bundesamts für Sicherheit in der Informationstechnik "in seiner Rolle als unabhängige und neutrale Beratungsstelle für Fragen der IT-Sicherheit"[10] wird in dem Entwurf nicht eingegangen. Der Entwurf sollte zumindest eine Prüfung unterschiedlicher Unabhängigkeitsmodelle vorsehen. [11]

Zu dem Mangel empirischer Evidenz bei der Normengestaltung[12] und fehlender Berücksichtigung der Vorgaben aus dem Koalitionsvertrag kommen weitere Defizite, auf die im Folgenden eingegangen wird. Eine weitere Überarbeitung des Referentenentwurfs wäre daher zielführend, um die Cyber- und Informationssicherheit in Deutschland nachhaltig zu stärken.

[7] Bundesanzeiger: Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz)
[8] Bundesregierung: Koalitionsvertrag zwischen CDU, CSU und SPD
[9] digitalcourage: Überwachungsgesamtrechnung
[10] Bundesregierung: Koalitionsvertrag zwischen CDU, CSU und SPD
[11] Sven Herpig: Die "Unabhängigkeit" des Bundesamtes für Sicherheit in der Informationstechnik
[12] Sven Herpig: Sachverständigenstellungnahme im Ausschuss des Deutschen Bundestags für Inneres und Heimat

B. Einzelkritik (nicht abschließend)

1. IT-Sicherheit für die Gesellschaft durch Verbraucherschutz

A. „Problem und Ziel“ in Verbindung mit „B. Lösung“ und Verweis auf §§ 3 und 9c BSIG-E

Der Entwurf definiert den Schutz von Gesellschaft als eines der Kernziele des Gesetzes. Als Hauptmaßnahme zum Schutz der Bürger:innen, und der damit verbundenen größten Personalaufwendung, führt der Entwurf die Einführung des „IT-Sicherheitskennzeichens“ an. Allerdings wird das IT-Sicherheitskennzeichen nicht direkt zu einer Erhöhung der IT- und Cybersicherheit in Deutschland führen. Eine indirekte Erhöhung der IT- und Cybersicherheit wäre bei verpflichtenden IT-Sicherheitssiegeln zumindest durch die Beeinflussung der Kaufentscheidung und des damit einhergehenden Einflusses auf Hersteller, die sich um eine verbesserte IT-Sicherheit ihrer Produkte bemühen müssten, gegeben.[13] Wenn eine Kennzeichnung mit dem IT-Sicherheitskennzeichen in Verbindung mit dem elektronischen Beipackzettel freiwillig ist, signalisiert es nur, wie (un)sicher ein Produkt ist. Weder die Produkte noch die Bürger:innen/Gesellschaft werden damit direkt sicherer. Zugespitzt bedeutet dies, dass IT-Produkte, deren Schutzmechanismen im Entwurf selbst als „faktisch wirkungslos“ bezeichnet werden, weiterhin verkauft werden dürften und nur auf Basis von Freiwilligkeit des Herstellers ein entsprechendes IT-(Un)Sicherheitskennzeichen auf der Verpackung tragen würden. Gleichzeitig entsteht durch die in §§ 9c und 3 Absatz 14 BSIG-E erwähnten Aufgaben ein hoher Mehraufwand für das Bundesamt für Sicherheit in der Informationstechnik. Es ist zu bezweifeln, dass der Ertrag den Aufwand beim freiwilligen IT-Sicherheitskennzeichen rechtfertigt. Die Maßnahme ist möglicherweise effektiv, aber keineswegs effizient. Vor dem Hintergrund der nach wie vor herrschenden Knappheit an IT-Sicherheitsfachkräften im öffentlichen Dienst sollte diese Maßnahme dringend überdacht werden.

Empfehlung: Die Bundesregierung sollte darauf hinarbeiten, dass bekanntermaßen unsichere und nicht mehr absicherbare IT-Produkte überhaupt nicht in den Handel gelangen dürfen.[14] Weiterhin sollten konkrete Maßnahmen ergriffen werden, die direkt für eine höhere Sicherheit der Bürger:innen sorgen, wie z. B. eine voreingestellte Netzwerksegmentierung bei Routern (Heimnetz/ IoT-Geräte). Die Idee des IT-Sicherheitskennzeichens sollte stattdessen direkt auf EU-Ebene angegangen werden, damit der Einsatz von verpflichtenden statt nur freiwilligen Siegeln ermöglicht werden kann (siehe „Warenverkehrsfreiheit“). Gleichzeitig muss sichergestellt werden, dass ein (freiwilliges) IT-Sicherheitskennzeichen nicht mit höherwertigen Zertifizierungen von Produkten vermischt wird.

[13] Philipp Morgner, Christoph Mai, Nicole Koschate-Fischer, Felix Freiling und Zinaida Benenson: Security Update Labels: Establishing Economic Incentives for Security Patching of IoT Consumer Products
[14] Verbraucherzentrale Nordrhein-Westfalen: Vorerst keine Sicherheit für Handynutzer: Urteil Oberlandesgericht Köln

2. Evaluierung der bisherigen IT- und Cybersicherheitsmaßnahmen

„A. Problem und Ziel“ in Verbindung mit „C. Alternativen“

Als sehr weit gefasste Zielvorgabe gibt der Entwurf vor, dass „die Gewährleistung der Cyber- und Informationssicherheit [ein] Schlüsselthema für Staat, Wirtschaft und Gesellschaft [ist]“. Eine Alternative zu allen im Entwurf vorgeschlagenen Normen wird nicht genannt. Es ist schwer nachvollziehbar, dass bei einer so umfassenden Zielvorgabe keine einzige Alternative genannt werden kann. Dies ist möglicherweise auf die fehlende Evaluierung der Effektivität der bisher implementierten staatlichen Maßnahmen zur Erhöhung der Cyber- und IT-Sicherheit in Deutschland zurückzuführen.

Empfehlung: Die Bundesregierung sollte die Effektivität der bisher getroffen Cyber- und IT-Sicherheitsmaßnahmen evaluieren und unter Einbeziehung der Expertise aus Wirtschaft, Wissenschaft und Zivilgesellschaft Alternativen entwerfen, bevor der vorliegende Gesetzestext als alternativlos bezeichnet wird.

3. Mobile Incident Response Teams

„E.3 Erfüllungsaufwand der Verwaltung“ in Verbindung mit § 5b BSIG-E

Die Mobile Incident Response Teams (MIRTs) des Bundesamtes für Sicherheit in der Informationstechnik sind ein Kernelement reaktiver Maßnahmen in der deutschen Cyber- und IT-Sicherheitspolitik. Der Mehrwert der MIRTs für die deutsche Cyber- und IT-Sicherheitspolitik ist für die Öffentlichkeit nachvollziehbar, wie u. a. der Fall des Lukaskrankenhauses in Neuss[15] gezeigt hat.

Empfehlung: Ein Ausbau der MIRTs ist zu unterstützen, da für diese eine breite Fachexpertise – zum Beispiel für die unterschiedlichen Systeme Kritischer Infrastrukturen – bereitgehalten werden muss. Der genannte Ausbau der Teams wäre eine effiziente Investition der im Entwurf insgesamt vorgesehenen Personalressourcen. Es ist dabei jedoch unklar, wie viele MIRTs notwendig sind, u. a. wegen Bereitschaftszeiten und Spezialexpertise. Es sollte daher dargelegt werden, welcher Plan hinter dem Ausbau der MIRTs steht und wie viele dieser Teams zu welchem Zeitpunkt für welche Einsatzgebiete (Regierung, KRITIS o. ä.) bereitstehen müssen. Dieser Plan sollte auch Transparenz über Einsatzstatus, Aufgabenteilung und Einsatzgebiete der „Quick Reaction Forces“ des Bundeskriminalamts, der „Mobile Cyber-Teams“ des Bundesamts für Verfassungsschutz und analoger Teams des Militärischen Abschirmdiensts und Bundesnachrichtendiensts herstellen.[16] Zudem sollte eine Einbettung des Konzepts des Cyber-Hilfswerks[17] in diesen Plan geprüft werden.

[15] Noah Gottschalk: Wenn eine Klinik ohne Computer arbeiten muss
[16] Bundesministerium des Innern: Cyber-Sicherheitsstrategie für Deutschland 2015
[17] AG KRITIS: Cyber-Hilfswerk (CHW)

4. Unternehmen im besonderen öffentlichen Interesse und Parteien

§ 2 Absatz 14 BSIG-E in Verbindung mit §§ 2 Absatz 3 Satz 2, 8, 8f und 10 Absatz 5 BSIG-E

Es ist unklar, in welchem Verhältnis die bestehenden „Institutionen im besonderen staatlichen Interesse" (INSI)[18] zu den im Entwurf erstmals erwähnten „Unternehmen im besonderen öffentlichen Interesse" gem. § 8f BSIG-E und der „Infrastruktur im besonderen öffentlichen Interesse“ gem. § 109a Abs 8 TKG-E stehen. Weder in der EU NIS-Richtlinie[19] noch in dem entsprechenden Umsetzungsgesetz[20] finden sich diese Begrifflichkeiten wieder. Im Umsetzungsgesetz wird lediglich einmal von „informationstechnischen Systemen von besonderem öffentlichem Interesse" gesprochen (§ 5a Absatz 2 BSIG). Diese Inkonsistenzen wirken einer Harmonisierung entgegen und verstärken die Komplexität durch die unilaterale Einführung einer weiteren „Schutzklasse“.

Empfehlung: Die Bundesregierung muss Transparenz bzgl. der „Institutionen im besonderen staatlichen Interesse“ im Vergleich zu „Unternehmen im besonderen öffentlichen Interesse“ schaffen. Gleichzeitig sollten die Kategorien der deutschen Gesetzgebung nicht von der EU-Harmonisierung abweichen, weshalb eine zusätzliche, unilaterale Einführung der „Unternehmen im besonderen öffentlichen Interesse“ o. ä. verworfen werden sollte. Auch inhaltlich erscheint diese zusätzliche Kategorie nicht sinnvoll: Entweder werden Unternehmen als kritisch genug betrachtet, um sie bzgl. IT-Sicherheit zu regulieren und folglich unter der KRITIS-Regulierung zu subsumieren, oder aber sie werden als nicht relevant genug eingeordnet, um bzgl. IT-Sicherheit reguliert zu werden. In diesem Fall können sie dann unter den bestehenden, unbestimmten Rechtsbegriff der „Institutionen im besonderen staatlichen Interesse“ fallen. Eine Ausdifferenzierung kann bei Aufnahme in die KRITIS-Regulierung über die branchenspezifischen Sicherheitsstandards[21] stattfinden.

Darüber hinaus ist zu prüfen, ob politische Parteien ab einer bestimmten Mitgliederanzahl wegen ihrer Relevanz für das Funktionieren des deutschen Staates in die KRITIS-Regulierung aufgenommen werden sollten.[22] Vor dem Hintergrund der Gewaltenteilung könnten alternativ Mindeststandards für die Sicherheit der Informationstechnik des Bundes gem. § 8 für Parteien empfehlenden Charakter haben, analog zu der Regelung für Gerichte und Verfassungsorgane nach § 2 Absatz 3 Satz 2.

Sollte die Bundesregierung an der Einführung der zusätzlichen Kategorie „Unternehmen im besonderen öffentlichen Interesse“ festhalten, so ist zumindest § 10 Absatz 5 BSIG-E um die Beteiligung der organisierten Zivilgesellschaft zu erweitern.

[18] Bundesamt für Sicherheit in der Informationstechnik: Allianz für Cyber-Sicherheit Registrierung
[19] Amtsblatt der Europäischen Union: RICHTLINIE (EU) 2016/1148 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 6. Juli 2016
[20] Bundesgesetzblatt: Gesetz zur Umsetzung der Richtlinie (EU) 2016/1148des Europäischen Parlaments und des Rates vom 6. Juli 2016
[21] Bundesamt für Sicherheit in der Informationstechnik: Branchenspezifische Sicherheitsstandards
[22] Sven Herpig und Julia Schuetze: Mehr IT-Sicherheit für deutsche Wahlen

5. Schwachstellenmanagement und -meldewesen

§ 4b BSIG-E in Verbindung mit §§ 7, 7a, 7b und 7c BSIG-E

Der Umgang mit Schwachstellen ist einer der wichtigsten Aspekte zur Herstellung von IT-Sicherheit in Unternehmen und Behörden. Klare Prozesse und Verantwortlichkeiten, die der technischen Komplexität Rechnung tragen, sind daher unbedingt notwendig. Die mit dem Entwurf geplante Regulierung bzgl. des staatlichen Schwachstellenmanagements und -meldewesens ist vollkommen intransparent. Es ist zu erwarten, dass diese Intransparenz zu ineffektiven Prozessen und einem Vertrauensverlust bei Firmen und IT-Sicherheitsforscher:innen -- Akteuren, die elementar für eine solche Policy sind -- führen wird.

Empfehlung: Empfohlen wird ein Verweis auf eine separate Verordnung o. ä., die den Umgang mit Schwachstellen durch Behörden dezidiert regelt, anstatt einer Regelung der Prozesse über die im Entwurf angeführten Normen. Zudem wird eine Einführung des seit Jahren in Planung befindlichen Schwachstellenmanagements des Bundesministeriums des Innern, für Bau und Heimat am Beispiel des von der Stiftung Neue Verantwortung vorgelegten Entwurfs empfohlen[23]. Gleichzeitig sollte ein Errichtungsgesetz für die Schwachstellen-verarbeitende Zentrale Stelle für Sicherheit in der Informationstechnik erarbeitet werden. Das ist dringend notwendig, da die Behörde ihre invasive Tätigkeit momentan ohne eine solche Gesetzesgrundlage ausübt. In den Gesetzen aller Schwachstellen-verarbeitenden Sicherheitsbehörden auf Bundesebene (u. a. Bundesnachrichtendienst, Bundeskriminalamt, Bundespolizei, Bundesamt für Verfassungsschutz, Bundeswehr, Zentrale Stelle für Sicherheit in der Informationstechnik) muss eine Reziprozität bzgl. der Weitergabe von Schwachstellen ergänzt werden: Während das Bundesamt für Sicherheit in der Informationstechnik gem. § 3 Absatz 1 Satz 13 BSIG andere Bundesbehörden bei der Wahrnehmung ihrer gesetzlichen Aufgaben unterstützen muss, sind diese Bundesbehörden ihrerseits nicht verpflichtet, das Bundesamt für Sicherheit in der Informationstechnik durch die Weitergabe der von ihnen gefundenen oder erworbenen Schwachstellen zu unterstützen. Dies ist allerdings eine Grundvoraussetzung für die Wahrnehmung der gesetzlichen Aufgaben des Bundesamtes für Sicherheit in der Informationstechnik.

Auch vor diesem Hintergrund wäre eine stärkere fachliche Unabhängigkeit des Bundesamtes für Sicherheit in der Informationstechnik vom Bundesministerium des Innern, für Bau und Heimat zielführend.

[23] Sven Herpig: Schwachstellen-Management für mehr Sicherheit

6. Untersuchung der Sicherheit in der Informationstechnik

§ 7a BSIG-E in Verbindung mit §§ 7, 7a, 7b und 7c BSIG-E

Die Norm enthält wenige Einschränkungen darüber, welche informationstechnischen Produkte und Systeme das Bundesamt für Sicherheit in der Informationstechnik untersuchen darf (Absatz 1). Darüber hinaus darf das Bundesamt für Sicherheit in der Informationstechnik in diesem Kontext alle notwendigen Informationen von den Herstellern einfordern (Absatz 2). Eine anlasslose Untersuchung aller informationstechnischen Produkte und Systeme mit einer zusätzlichen Befugnis, externe Informationen anzufordern, ist sehr breit. Gleichzeitig werden dem Bundesamt kaum Beschränkungen auferlegt, wie es mit den so erworbenen Informationen verfahren darf (Verweis auf die sehr breite Norm § 3 Absatz 1 Satz 2 BSIG). Dies könnte folglich auch die Weitergabe von Informationen zu Schwachstellen an andere Sicherheitsbehörden beinhalten, welche die Schwachstellen ausnutzen und damit dem gesetzlichen Auftrag des Bundesamtes für Sicherheit in der Informationstechnik zuwiderhandeln würden.

Empfehlung: Zusätzlich zu den unter „5. Schwachstellenmanagement und -meldewesen“ genannten Empfehlungen sollte aufgrund der vorausgegangenen Analyse eine defensive Zweckbindung der so erlangten Informationen über die IT-Produkte und Systeme eingefügt werden (Absätze 2, 3 und 4). Zusätzlich sollte eine weitere Verengung der Norm geprüft werden.

7. IT-Sicherheit in Digitalisierungsvorhaben

§ 8 Absatz 4 BSIG-E

Die Zeitangabe “frühzeitig” im Kontext der Einbindung des Bundesamtes für Sicherheit in der Informationstechnik in Digitalisierungsvorhaben des Bundes wird in dieser Norm nicht näher definiert. Zusätzlich ist das Bundesamt für Sicherheit in der Informationstechnik gegenüber dem Bundesministerium des Innern, für Bau und Heimat fachlich weisungsgebunden und das Ministerium muss über jede Zusammenarbeit des Bundesamts für Sicherheit in der Informationstechnik informiert werden (vgl. § 26 GGO). Vor dem Hintergrund dieser Beschränkungen führt die Norm wahrscheinlich nicht zu der beabsichtigten früheren Einbindung des Bundesamts für Sicherheit in der Informationstechnik in Digitalisierungsvorhaben der Bundesverwaltung.

Empfehlung: Die Angabe „frühzeitig“ sollte präzisiert bzw. ein grober Zeitraum inkludiert werden. Weiterhin sollte ermöglicht werden, dass andere Behörden die Unterstützung des Bundesamts für Sicherheit in der Informationstechnik direkt und ohne vorherigen Kontakt zum Bundesministerium des Innern, für Bau und Heimat ersuchen können. Das würde auch die im Koalitionsvertrag angekündigte Stärkung des Bundesamts für Sicherheit in der Informationstechnik "in seiner Rolle als unabhängige und neutrale Beratungsstelle für Fragen der IT-Sicherheit"[24] fördern.

[24] Bundesregierung: Koalitionsvertrag zwischen CDU, CSU und SPD

8. Kritische Komponenten und vertrauenswürdige Hersteller

§ 9b BSIG-E in Verbindung mit § 2 Absatz 13 BSIG-E

Die sehr breite Definition von „kritischen Komponenten“ in Verbindung mit der Garantieerklärung über die „gesamte Lieferkette des Herstellers“ auf Basis einer nicht näher definierten späteren Allgemeinverfügung des Bundesministeriums des Innern, für Bau und Heimat macht eine Bewertung dieser Norm ohne weitere Details schwer möglich. Der Anwendungsbereich dieser Norm geht weit über die technische IT- und Cybersicherheit hinaus, für die das Bundesamt für Sicherheit in der Informationstechnik – und damit das BSIG – verantwortlich ist. Dies wird unter anderem dadurch deutlich, dass in diesem Kontext das Bundesministerium des Innern, für Bau und Heimat und nicht mehr das Bundesamt für Sicherheit in der Informationstechnik genannt wird. Diese Perspektive wird dadurch verstärkt, dass sowohl die Inhalte der Garantieerklärung als auch die Risikobewertung des Herstellers der kritischen Komponente „im Einvernehmen mit den jeweils betroffenen Ressorts erfolgen“. Weiterhin soll zur Unterstützung ein fortlaufender Austausch durch einen „interministeriellen Jour Fixe […] (BMI, BMWi, AA, Bundeskanzleramt auf Ebene Referatsleitung)“ sichergestellt werden. Die Grundlage für eine fortlaufende, interministerielle Bewertung des Risikoprofils eines Herstellers, u. a. hinsichtlich „Organisationsstruktur […] Handlungen […] rechtlichen Verpflichtungen“ sollte jedoch nicht im BSIG-E gelegt werden. Gleichzeitig ist eine solche interministerielle Bewertung unter Einbeziehung sicherheitspolitischer Belange essenziell.

Hinsichtlich zukünftiger Telekommunikationsnetze muss auch grundsätzlich in Frage gestellt werden, inwieweit das geplante Vorgehen flexibel und responsiv genug ist, um Risiken in zunehmend software-definierten Netzwerken adäquat zu adressieren:

1. „Kritische Komponenten“ müssen zunächst durch den Katalog von Sicherheitsanforderungen nach § 109 Absatz 6 TKG näher bestimmt werden.
2. Kritische Komponenten „dürfen nur eingesetzt werden, wenn sie von einer anerkannten Prüfstelle überprüft und von einer anerkannten Zertifizierungsstelle zertifiziert wurden“ (§ 109 Absatz 2 TKG).
3. Betreiber müssen vor dem Einsatz einer kritischen Komponente zusätzlich eine Garantieerklärung des Herstellers beim Bundesministerium des Innern, für Bau und Heimat vorlegen.
4. Innerhalb eines Monats prüft das Bundesministerium des Innern, für Bau und Heimat die Garantieerklärung, u. a. basierend auf der Arbeit im interministeriellen Jour Fixe, und genehmigt oder untersagt den Einsatz.

5G-Netze sind zunehmend software-definiert, d. h. „kritische Komponenten“ sind meist Softwarekomponenten, deren Funktionalität zügig angepasst werden kann. Dieser zentrale Aspekt moderner Telekommunikationsnetze bleibt jedoch weitestgehend unberücksichtigt durch den engen Fokus auf Zertifizierung kritischer Komponenten. Bürokratische Kosten und Nutzen für die tatsächliche IT-Sicherheit unserer Telekommunikationsnetze stehen hier in einem schlechten Verhältnis.

Empfehlung: Die Norm § 9b BSIG-E sollte ersatzlos gestrichen und in ein separates Gesetzesvorhaben überführt werden.

9. Eingriff der Diensteanbieter in die Integrität von Kundensystemen

§ 7c BSIG-E Absatz 1 Satz 2 in Verbindung mit § 109a TKG Absätze 4,5 und 6

Es handelt sich hierbei um einen angeordneten Eingriff in das Computergrundrecht[25]. Es ist unklar, wie die operative Umsetzung aussähe und welche Schutzmechanismen ergriffen würden, um die Verfügbarkeit und Vertraulichkeit der betroffenen Datenverarbeitungssysteme durch die Veränderung der Integrität nicht zu beeinträchtigen. Darüber diese Maßnahme im Sinne der IT- und Cybersicherheit keinen erkennbaren zusätzlichen Schutz zu den Maßnahmen gem. TKG § 109a Absätze 4, 5 und 6.

Empfehlung: § 7c BSIG-E Absatz 1 Satz 2 sollte ersatzlos gestrichen werden.

10. Anordnungsbefugnis gegenüber Diensteanbietern

§ 7d BSIG-E

Es handelt sich hierbei um eine unpräzise gefasste Norm (Beispiel: „Vielzahl von Nutzern“). Dies ist vor dem Hintergrund eines möglicherweise hohen Erfüllungsaufwands problematisch.

Empfehlung: Diese Norm sollte weiter präzisiert werden.

11. Pflichten der Diensteerbringer

§ 15b Absatz 1 TMG-E

Es handelt sich hierbei um eine zu weitgefasste Norm, die unter anderem auf einer unklaren Begründung des Staatswohls – vgl. § 15b Abs 1 Satz 3 TMG-E – basiert. Problematisch ist weiterhin, dass keine Bereichsausnahmen für Tätigkeiten im öffentlichen Interesse, zum Beispiel für die Arbeit der Presse, vorgesehen sind. Es ist anzuzweifeln, dass Diensteerbringer in der Vergangenheit einer entsprechenden Verpflichtung gem. § 15b Abs 1 TMG-E wissentlich nicht gefolgt sind. Weiterhin stellt § 15b Abs 2 TMG-E ohne Anordnung durch zuständige Behörden, zum Beispiel durch das Bundeskriminalamt, einen möglicherweise unverhältnismäßigen Aufwand für die Diensteerbringer dar.

Empfehlung: Es ist zu prüfen, ob eine empirische Grundlage für § 15b Abs 1 TMG-E gewährleistet ist, gemäß derer Diensteerbringer dieser Pflicht nicht nachgekommen sind. § 15b Abs 2 TMG-E sollte ausschließlich eine zwingende und nicht optionale Anordnung der zuständigen Stellen vorsehen. Die Norm sollte um § 15b Abs 4 TMG-E ergänzt werden, der eine Ausnahme von den Absätzen 1-3 vorsieht, sobald die zur Veröffentlichung vorgesehenen Daten dem öffentlichen Interesse dienen. Dies sollte insbesondere dann gelten, wenn das Handeln im Einklang mit § 5 GeschGehG und dem geltenden Datenschutzrecht, sowie den hierin enthaltenen Bereichsausnahmen medialer Arbeit (beispielhaft: § 12 LPG NRW, § 59 RStV) steht.

[25] Bundesverfassungsgericht: Leitsätze zum Urteil des Ersten Senats vom 27. Februar 2008- 1 BvR 370/07 -- 1 BvR 595/07 -

12. Sonderrolle von Auswärtigem Amt und Bundeswehr

§ 4a BSIG-E Absätze 5 und 6 in Verbindung mit § 8 BSIG-E Absatz 1a und „Begründung", „Besonderer Teil"

Mit § 4a BSIG-E werden zusätzliche Befugnisse geschaffen, damit das Bundesamt für Sicherheit in der Informationstechnik die IT-Sicherheit der Kommunikationstechnik des Bundes erhöhen kann. Die Begründung warum gem. der Absätze 5 und 6 (Teile der) Informations- und Kommunikationsstruktur der Bundeswehr und das Auswärtige Amt hiervon ausgenommen werden sollen ist aus IT-Sicherheitsperspektive schwer nachvollziehbar. Die Befugnisse des Bundesamtes für Sicherheit in der Informationstechnik sollen individuell über Verwaltungsvereinbarungen zwischen dem Bundesministerium der Verteidigung und dem Bundesministerium des Innern, für Bau und Heimat respektive dem Auswärtigen Amt und dem Bundesministerium des Innern, für Bau und Heimat geregelt werden, was die Transparenz einschränkt. Zusätzlich sollen Teile des Bundesministeriums der Verteidigung gem. §8 BSIG-E Absatz 1a von der Kontrolle und Überwachung des Mindeststandards für Sicherheit in der Informationstechnik des Bundes ausgenommen werden.

Während die Ausnahmeregelung gem. § 4a Absatz 6 für die Bundeswehr – u. a. auf Basis der eigenen IT-Fähigkeiten im Organisationsbereich Cyber- und Informationsraum – nachvollziehbar erscheint, ist die Ausnahme des Auswärtigen Amts gem. § 4a Absatz 5 unverständlich und ggf. gefährlich. Das liegt sowohl an den, im Gegensatz zur Bundeswehr, begrenzteren eigenen IT-Fähigkeiten, sowie der Homogenität der IT-Systeme (z. B. keine Wehrtechnik), als auch – wie im Referentenentwurf beschrieben – Cyberoperationen gegen das Ministerium. Gerade die Ausnahme des Auswärtigen Amtes wäre auf dieser Basis ein falsches Zeichen für die IT-Sicherheit in Deutschland.

Empfehlung: §4a BSIG-E Absatz 5 sollte ersatzlos gestrichen werden, zumindest aber sollte die Verwaltungsvereinbarung öffentlich gemacht werden müssen. §4a BSIG-E Absatz 6 müsste in der Begründung umfassender erklärt werden und die Verwaltungsvereinbarung sollte öffentlich gemacht werden müssen. Zu §8 BSIG-E Absatz 1a letzter Satz sollte wie folgt abgeändert werden: „Im Geschäftsbereich des Bundesministeriums der Verteidigung sind die Mindeststandards für Informations- und Kommunikationstechnik im Sinne des § 4a Absatz 6 grundsätzlich umzusetzen. Nur begründet im Verteidigungsauftrag nach vorhergehender Risikoanalyse sind hier individuelle Ausnahmen möglich".

13. Staatliche Cybersicherheitsarchitektur

„Begründung", „Allgemeiner Teil", „VI. Gesetzesfolgen", „2. Nachhaltigkeitsaspekte"

Der Referentenentwurf betrachtet die notwendige Reform der offensichtlich dysfunktionalen, zentralen Akteure der deutschen Cybersicherheitsarchitektur, dem Nationalen Cyber-Abwehrzentrum und dem Cyber-Sicherheitsrat nicht.

Empfehlung: Das IT-Sicherheitsgesetz 2.0 sollte genutzt werden, um die Strukturen des Nationalen Cyber-Abwehrzentrums und des Cyber-Sicherheitsrats zu klären und eine rechtliche Grundlage für die Arbeit dieser Institutionen, und der Zentralen Stelle für Informationstechnik im Sicherheitsbereich, zu

schaffen. Dies sollte unter anderem Kooperationsmöglichkeiten und -grenzen, Verantwortlichkeiten, Aufgaben und Verortung in der deutschen Cybersicherheitsarchitektur beinhalten. Hierzu gehört beispielsweise die Trennung zwischen operativen und nicht operativen Aufgaben im Bereich der Cybersicherheit (vgl. u. a. BVerfG Leitsätze zum Urteil des Ersten Senats vom 19. Mai 2020)[26]. Weiterhin sollte die Bundesregierung einen Plan zu Weiterentwicklung der deutschen Cybersicherheitsarchitektur vorlegen, insbesondere vor dem Hintergrund der Gründung immer neuer Institutionen wie der Zentralen Stelle für Sicherheit in der Informationstechnik, der Agentur für Sprunginnovationen, der Cyberagentur, dem Zentrum für Digitalisierungs- und Technologieforschung der Bundeswehr und vielen mehr, und damit möglicherweise entstehender unklarer Verantwortlichkeiten und Parallelstrukturen entgegenwirken.

C. Zusammenfassung

Durch die Weiterentwicklung der Gefährdungslage seit dem letzten IT-Sicherheitsgesetz ist es dringend geboten die IT-Sicherheitsgesetzgebung weiter zu verbessern. Aufgrund der bevorstehenden Bundestagswahlen 2021 wäre es für die IT-/Cybersicherheit in Deutschland wichtig eine entsprechende Gesetzgebung noch im ersten Halbjahr 2021 zu verabschieden. Wie dargestellt beinhaltet der vorliegende Entwurf jedoch noch elementare Schwächen und bedarf weiterer Überarbeitung. Folgendes Vorgehen würde aus hiesiger Sicht daher den kleinsten gemeinsamen Nenner darstellen:

Die Übernahme folgender Empfehlungen in den Gesetzestext ist notwendig:

„8. Kritische Komponenten und vertrauenswürdige Hersteller“

„9. Eingriff der Diensteanbieter in die Integrität von Kundensystemen“

„11. Pflichten der Diensteerbringer“

„12. Sonderrolle von Auswärtigem Amt und Bundeswehr“

Die Übernahme folgender Empfehlungen kann in der Cybersicherheitsstrategie 2021 erfolgen:

„2. Evaluierung der bisherigen IT- und Cybersicherheitsmaßnahmen“

„13. Staatliche Cybersicherheitsarchitektur“

Die Übernahme folgender Empfehlung kann durch Einführung eines staatlichen Schwachstellenmanagements in 2021 erfolgen:

„5. Schwachstellenmanagement und -meldewesen“

Die Übernahme folgender Empfehlungen kann 2021 auf EU-Ebene erfolgen:

„1. IT-Sicherheit für die Gesellschaft durch Verbraucherschutz“

„4. Unternehmen im besonderen öffentlichen Interesse und Parteien“

[26] Bundesverfassungsgericht: Leitsätze zum Urteil des Ersten Senats vom 19. Mai 2020 - 1 BvR 2835/17 – [5. Leitsatz]

Von:	Manuel Atug <honkhase@ag.kritis.info>
Gesendet:	Donnerstag, 3. Dezember 2020 11:04
An:	sprecher@ag.kritis.info
Betreff:	Stellungnahme der AG KRITIS zum dritten Entwurf des IT-Sicherheitsgesetz 2.0
Anlagen:	AG-KRITIS-Stellungnahme-IT-SiG2-RefE3.pdf

Deutscher Bundestag
Ausschuss für Inneres und Heimat
Ausschussdrucksache
19(4)664

Sehr geehrte Damen und Herren,

anbei senden wir Ihnen die beiliegende dringliche Stellungnahme zum dritten Entwurf des IT-Sicherheitsgesetz 2.0.

Die AG KRITIS fordert die Notbremse für den ITSiG2-Gesetzesentwurf. Nicht nur zeigt dieser Entwurf, dass er von fachfremden Personen mit der heißen Nadel gestrickt wurde - auch finden sich dort Formulierungen, welche die Krisenreaktionsfähigkeit des BSI verlangsamen. Zusätzlich verstrickt sich das BMI in Widersprüche in Bezug auf die Vorhaltung von nutzlosen Logdaten und darüber hinaus muss sogar die Zustimmung von Sicherheitsbehörden eingeholt werden, bevor KRITIS-Betreiber über schwerwiegende Sicherheitslücken informiert werden dürfen.

Und damit nicht genug: Teile der Aufgaben von Staatsanwaltschaften werden ohne Richtervorbehalt an Telekommunikationsanbieter ausgelagert und werden so privatisiert.
Dieses Gesetz ist auf fraglichen Grundlagen im luftleeren Raum entstanden und kann nur auf dem fehlgeleiteten Bauchgefühl einzelner BMI-Mitarbeiter basieren, da die gesetzlich vorgesehene Evaluierung des ersten IT-SiG weiterhin nicht vorgenommen wurde und weiterhin aussteht. Die unüblich kurze und dialogfeindliche Fristsetzung zur Kommentierung unterstreicht die Unangemessenheit des Erstellungsprozesses.

Zur Einschätzung, dass dieser Gesetzesentwurf gestoppt werden muss, kommt die AG KRITIS, nachdem Sie eine umfassende Stellungnahme auf ihrer Website veröffentlicht hat, in der alle kritischen Änderungen analysiert und diskutiert werden. Vor dem Hintergrund, dass laut netzpolitik.org dieses Gesetz schon am 16.12.2020 durch das Kabinett beschlossen werden soll, sehen wir keine Möglichkeit mehr, dass Korrekturen im notwendigen Umfang stattfinden könnten. Daher ist ein sofortiges Ziehen der Notbremse durch die zuständigen Minister nun zwingend notwendig.

Die AG KRITIS ist ein unabhängiger, ehrenamtlicher Zusammenschluss von über 40 Experten, die sich täglich mit Kritischen Infrastrukturen (KRITIS) gemäß § 2 (10) BSI-Gesetz i. V. m. BSI-Kritisverordnung beschäftigen, z. B. durch Planung, Bau, Betrieb, Beratung oder Prüfung der beteiligten IT-Systeme und Anlagen. Die Arbeitsgruppe ist vollständig unabhängig von Staat oder Wirtschaft. Wir vertreten keine Interessen von Unternehmen oder Wirtschaftsverbänden, sondern unser Ziel ist es einzig und allein, die Versorgungssicherheit der Bevölkerung zu erhöhen.

Die Stellungnahme ist auch auf der Website der AG KRITIS veröffentlicht:
https://ag.kritis.info/2020/12/03/notbremse-fuer-den-entwurf-stellungnahme-der-ag-kritis-zum-3-entwurfs-des-it-sig-2-0/

Für Rückfragen oder weitere Informationen stehen wir Ihnen zur Verfügung.

Beste Grüße aus Bonn,

Manuel Atug
Gründer und Sprecher der AG KRITIS

https://ag.kritis.info/
https://twitter.com/AG_KRITIS

Saarbrückener Str. 115

Berlin, 03.12.2020

Notbremse für den Entwurf! - Stellungnahme der AG KRITIS zum 3. Entwurfs des IT-SiG 2.0

Am 21.11.2020 haben wir den dritten Referentenentwurf des IT-Sicherheitsgesetzes 2.0 in unserem Blog veröffentlicht. Den nun am 02.12.2020 durch das Bundesministerium des Inneren, für Bau und Heimat veröffentlichten Entwurf entspricht dieser Vorabversion mit nur geringfügigen Änderungen. Neben einigen Verbesserungen enthält der Gesetzesentwurf jedoch auch eine Reihe an erheblichen Mängeln, welche wir als sehr problematisch einschätzen. Auf Grund der zu kurzen Frist zur Stellungnahme und der laut netzpolitik.org geplanten Verabschiedung am 16. Dezember 2020 durch das Kabinett halten wir es für ausgeschlossen, dass notwendige Änderungen noch Einzug in den Gesetzesentwurf finden können.

Wir fordern daher einen **Aufschub des Gesetzgebungsverfahrens** und eine **echte Einbindung der** zahlreichen **zivilgesellschaftlichen und sonstigen Organisationen**, die sich mit der Cyber-Sicherheitspolitik beschäftigen.

Nicht erkennbare Strategie im dritten IT-SiG 2.0 - Entwurf

Der vorgelegte Gesetzesentwurf lässt keine klare Linie zur konsequenten Erhöhung des Sicherheitsniveaus der IT und Kritischen Infrastrukturen erkennen. Im gesamten Gesetzestext ist keine Strategie erkennbar, grundlegende Sicherheitsanforderungen zu stärken. Vielmehr scheint es sich um eine bunte Mischung - teilweise sachfremder - Wünsche seitens einzelner Behörden zu handeln. Grundlegende Maßnahmen, die sinnvoll wären, wie die verpflichtende Einführung eines Informationssicherheitsmanagementsystems (ISMS) sind nicht enthalten. Gute Ideen aus vorherigen Entwürfen fehlen nun ganz, dafür wurden mehrere verfassungsrechtlich höchst fragliche Passagen hinzugefügt.

Inhaltsverzeichnis

Notbremse für den Entwurf! - Stellungnahme der AG KRITIS zum 3. Entwurfs des IT-SiG 2.0.....1
Nicht erkennbare Strategie im dritten IT-SiG 2.0 - Entwurf.....1
Gesetzesanpassungen mit Bauchgefühl statt Evaluierung.....3
Thema verfehlt: verpflichtende Systeme zur Angriffserkennung.....3
Anonym und überflüssig: Speicherung von Protokolldaten.....4
Logdaten von KRITIS-Betreibern.....4
Logdaten von Kommunikationstechnik des Bundes.....5
UNBÖFI - Es braucht kein "KRITIS light".....5
Rüstungsindustrie via Außenwirtschaftsverordnung.....5
Änderung an den Sektoren.....7
Keine Krisenreaktionspläne und keine BBK-Stärkung.....7
Offensive Maßnahmen gegen IT-Grundrechte.....8
Übertragung von Aufgaben der Staatsanwaltschaften auf Diensteanbieter.....8
Umgehung des Nationalen Cyber Abwehrzentrum (NCAZ).....9
Unterlassene Hilfeleistung: Fehlende Warnung von Betreibern.....9
Scanning-Befugnisse des BSI zu eng gefasst.....9
Unterlassung von Warnungen an KRITIS Betreiber sind intolerabel.....10
Vertrauenswürdige Hersteller - Lex Huawei für KRITIS?.....11
Resilienz kommt zu kurz: Kritische Infrastruktur vs. Kritische Komponenten.....12
Keine Änderung an Strafprozessordnung und am Strafgesetzbuch.....12
Herausgabe von Informationen zur Bewältigung einer erheblichen Störung.....13
KRITIS bekommt Zähne: erhöhte BSI Bußgelder.....13
Deutscher Alleingang: IT-Sicherheitskennzeichen.....13
Vorherige Stellungnahme der AG KRITIS.....14

Gesetzesanpassungen mit Bauchgefühl statt Evaluierung

Die gesetzlich festgelegte Evaluierung des IT-SIG 1.0 gemäß Artikel 10 "*unter Einbezug eines wissenschaftlichen Sachverständigen, der im Einvernehmen mit dem Deutschen Bundestag bestellt wird*" steht weiterhin aus. Auch laut § 9 KritisV muss die BSI-Kritisverordnung - und damit insbesondere auch die Schwellwerte, ab denen ein Betreiber als Kritische Infrastruktur betrachtet wird - alle zwei Jahre evaluiert werden. Diese Evaluierungen wurden inzwischen wiederholt versäumt.

Die zuvor genannte Evaluierung ist allerdings ein elementarer Bestandteil zur Prüfung der Wirksamkeit und muss durchgeführt werden, bevor eine Kompetenz- und Anforderungsausweitung mit dem neuen IT-SiG 2.0 vorgenommen wird. Stattdessen wird die Pflicht zur regelmäßigen Evaluierung mit diesem Entwurf vollständig entfernt.

Es ist darüber hinaus mehr als bedenkenswert, dass nun bzw. erst im Dezember 2020 die Stellungnahme von Interessensvertretungen, Verbänden und der Zivilgesellschaft erfolgen kann und ohne hinreichende Konsultationsfrist (vom 2. Dezember bis 6. Dezember, dann verlängert bis 9. Dezember, also nur 5 Werktage) eine unvollständige sowie nicht-zielführende Gesetzesänderung beschlossen werden soll. Eine Frist von nur einer Woche kann nicht dem demokratischen Gedanken entsprechen und spiegelt nicht die Wichtigkeit der geplanten Gesetzesanpassungen wider.

Die Kernidee des Schutzes kritischer Infrastrukturen kommt viel zu kurz. Stattdessen werden sachfremde Themen eingebracht. Vorhandene Möglichkeiten, die Unzulänglichkeiten bisheriger Gesetze zu beheben, konnten nicht genutzt werden, weil aufgrund der gesetzwidrig unterlassenen Evaluationen keine eigenen Informationen im BMI dazu vorlagen.

Thema verfehlt: verpflichtende Systeme zur Angriffserkennung

Artikel 12, Seite 15 - Änderungen an § 8a Absatz 1, 1a, 1b... BSI § 8a 1b), EnWG § 11 1d)

Über den bestehenden § 8a BSIG ist bereits jetzt die Umsetzung eines ISMS und damit einhergehend eine Risikoanalyse mit anschließender Definition der Maßnahmen vorgegeben. Sofern sich hieraus ergibt, dass die Einführung und der Betrieb von Systemen zur Angriffserkennung (IDS oder IPS) als spezifische Maßnahme erforderlich ist, wird dieses bereits dadurch verpflichtend.

Die gesetzliche Vorgabe einzelner technischer Maßnahmen in einem Gesetz, wie z.B. einem IDS oder IPS, vollkommen unabhängig von einer Risikoanalyse der konkreten technischen Infrastruktur, ist nicht sinnvoll. Im Zweifel führt dies zu überflüssigen Aufwand und bindet Ressourcen die im Einzelfall bei wichtigeren Maßnahmen notwendig wären. Darüber hinaus ist

es unüblich, eine technische Maßnahme in dieser Konkretheit im Gesetz vorzugeben. Wenn überhaupt nötig, könnten Vorgaben auf einem solchen Detaillevel für einzelne Anlagenkategorien differenziert als Rechtsverordnung in der Kritis-Verordnung vorgegeben werden.

Anonym und überflüssig: Speicherung von Protokolldaten

Logdaten von KRITIS-Betreibern

§ 8a Absatz 1b BSIG

Eine Anonymisierung von Logdateien in Verbindung mit gleichzeitiger Umsetzung eines ISMS ist technisch ohne Duplizierung von Daten unmöglich. Es muss grundsätzlich davon ausgegangen werden, dass anonymisierte Logdateien nicht dem Stand der Technik zur Detektion und Reaktion auf Sicherheitsvorfalle im Rahmen des ISMS entsprechen. Ein Betreiber muss grundsätzlich in der Lage sein, Handlungen konkreten Personen zuzuordnen. Die Verpflichtung Logdaten zu speichern widerspricht zumindest für den Sektor Energie den Anforderungen, die aus dem Sicherheitskatalog der BNetzA abgeleitet werden können, denn im Sicherheitskatalog wird ein ISMS mit entsprechenden Maßnahmen gefordert.

Da eine IP-Adresse nach Einschätzung des Bundesbeauftragten für den Datenschutz in der Informationstechnik (BfDI) ein personenbezogenes Datum ist und daher diese Information entfernt werden müsste, ist der entstehende Datenhaufen nicht verwendbar und enthält keine Aussagekraft mehr.

> *Begründung dieser Änderung: "Eine Schätzung des Erfüllungs-Aufwands, im Wesentlichen die Kosten für die Systeme zur Angriffserkennung selbst sowie Personal, ist insoweit nicht möglich. Denn zum einen sind solche Systeme teilweise bereits bei Betreibern Kritischer Infrastrukturen im Einsatz, sodass für diese Betreiber durch die Neuregelung überhaupt keine zusätzlichen Kosten entstehen. Zum anderen sind die Kosten für diese Systeme sehr unterschiedlich."*

Das BMI sagt in der Begründung, das die Schätzung des Erfüllungsaufwands nicht möglich sei - denn solche Systeme seien ja bereits im Einsatz. Dabei übersieht das BMI, dass bei Betreibern viele Gigabyte, in manchen Fällen sogar Terabytes, pro Tag an Logdaten entstehen - diese Datenmenge für vier Jahre zu speichern lässt enorme Mehrkosten bei allen Betreibern entstehen und erzeugt aufgrund der vorgeschriebenen Anonymisierung keinen Mehrwert. Eine Analyse solcher Datenmengen ist extrem rechenaufwendig. Es ist fraglich, ob am Markt verfügbare Großcomputer in der Lage sein können, Logdateien dieser Größenordnung innerhalb angemessener Zeit - während eines Angriffs in der Regel nur Stunden oder weniger - auszuwerten. Schon der Transfer solcher Datenmengen zu einer entsprechenden

Großrechenanlage würde Wochen benötigen und einen erheblichen logistischen Aufwand mit sich bringen.

Diese Änderung belegt die Realitätsferne des zuständigen Referats im BMI - keiner der Mitarbeiter hat wohl jemals Logdaten eines KRITIS-Betreibers gesehen oder Informationen über den Prozess der Auswertung erlangt, ansonsten wäre diese Formulierung so nicht entstanden.

Logdaten von Kommunikationstechnik des Bundes

§ 5 Absatz 2 BSIG

Die Erweiterung der Speicherfrist von Logdaten aus dem Betrieb der Kommunikationstechnik des Bundes in von drei auf zwölf Monate begrüßen wir trotzdem - aufgrund der bisher rückständigen Digitalisierung der Bundesbehörden ist das Problem der zu großen Menge an Logdaten auf absehbare Zeit dort zumindest nicht zu befürchten - auch zeigen vergangene Angriffe auf Bundesbehörden wie z.B. den Bundestag, dass diese erst nach deutlich mehr als drei Monaten detektiert werden - hier benötigt es also die erweiterte Speicherdauer, um einen Angriff im Nachhinein noch nachvollziehen zu können.

UNBÖFI - Es braucht kein "KRITIS light"

Neuschaffung des § 8f BSIG

Die Unternehmen in besonderem öffentlichen Interesse (UNBÖFI), ehem. ISBÖFI stellen eine Art KRITIS-light da, die unnötig sind.

Rüstungsindustrie via Außenwirtschaftsverordnung

„Man muss Gesetze kompliziert machen, dann fällt es nicht so auf“, sagte Bundesinnenminister Horst Seehofer im Juni 2019. An dieses Mantra hält man im BMI wie gewohnt auch im IT-SiG 2.0 konsequent fest. Im Entwurf von 2019 fand sich noch die Formulierung, dass die Rüstungsindustrie zur sog. ISBÖFI, jetzt UNBÖFI gehören soll. Die „UNBÖFI“ ist quasi eine Art „KRITIS light“. Nicht alle KRITIS Pflichten werden auferlegt, aber manche. Im aktuellen IT-SiG2-Entwurf findet sich das Wort „Rüstung“ weiterhin nicht mehr, trotzdem gehört Rüstung weiterhin zu UNBÖFI. Dies wird durch die verschleiernde Erwähnung des „§ 60 AWV Absatz 1 Satz 1-5“ festgelegt und auch in den Begründungen zum Gesetz weder erläutert noch aufgeklärt.

Die Rüstungsindustrie ist weder KRITIS, noch kann sie zu einer Art „KRITIS light“ gehören - denn die Rüstungsindustrie gehört eben nicht zu solchen Diensten *„die von wesentlicher Bedeutung für die Aufrechterhaltung wichtiger gesellschaftlicher Funktionen, der Gesundheit, der*

Sicherheit und des wirtschaftlichen oder sozialen Wohlergehens der Bevölkerung sind und deren Störung oder Zerstörung erhebliche Auswirkungen hätte“. (KRITIS-Definition aus der EU NiS Richtlinie).

Die Rüstungsindustrie bedient allerdings militärische Bedürfnisse. Daher hat sie nichts in einem zivilen IT-Sicherheitsgesetz als "KRITIS light" zu suchen, wo aus der eigentlich erforderlichen Sicht der nationalen Sicherheit viel zu handzahme Vorgaben vorgesehen werden. Der aus staatlicher Sicht sogar begrenzt nachvollziehbare Wunsch, der Rüstungsindustrie höhere Auflagen für Resilienz in ihrer IT-Infrastruktur aufzuerlegen, kann nicht über die UNBÖFI-Gesetzgebung erfüllt werden. Die Rüstungsindustrie soll auch im Spannungs- und Verteidigungsfall noch funktionieren können. Dies erfordert grundlegend andere Vorgehensweisen und Maßnahmen, als die vorhandenen UNBÖFI-Vorgaben hergeben. Die Rüstungsindustrie gehört daher in das Weißbuch des Verteidigungsministeriums und im IT-SiG konsequent gestrichen.

Wir kritisieren, dass die genauen Kriterien nach denen ein Unternehmen "UNBÖFI" wird, nicht im Gesetz stehen, sondern durch Rechtsverordnung festgelegt werden.

Unternehmen im besonderen öffentlichen Interesse werden im Referentenenwurf des IT-SiG 2.0 in drei Unterkategorien unterteilt: (§ 2 Absatz 14 Satz)

1. sicherheitsrelevante Unternehmen (Rüstung / IT-Sicherheitstechnik für die Bundesrepublik)
2. volkswirtschaftlich relevante Unternehmen (gemäß inländischer Wertschöpfung, in einer Verordnung genauer zu definieren)
3. potenziell umwelt- / gesundheitsgefährdende Unternehmen (die unter die Störfallverordnung, Betriebsbereich oberer Klasse fallen)

Unternehmen nach Satz 2, also volkswirtschaftlich relevante Unternehmen, sollen durch das neue Gesetz nun auch die Möglichkeit haben unter Umständen unter eine Art KRITIS-light (UNBÖFI) zu fallen - dies stellt eine Ungleichbehandlung gegenüber kleineren Unternehmen dar. Auch ging es bisher um die Sicherstellung der Versorgung der Bevölkerung mit grundlegendsten Dienstleistungen - und eben nicht um die volkswirtschaftliche Wertschöpfung. Diese Änderung am Prinzip der KRITIS-Gesetzgebung ist so nicht sinnvoll und weicht die Trennschärfe der Regelung insgesamt auf.

Änderung an den Sektoren

§ 2 Absatz 10 BSIG

Wir begrüßen die Aufnahme von Siedlungsabfallentsorgung als neuen Kritische Infrastruktur Sektor. Weiterhin fehlt allerdings der Sektor Chemie. Für diesen werden zwar in der Störfall-Verordnung diverse Vorsichtsmaßnahmen zum Schutz vor Unfällen festgelegt, der Bereich der Prozessleittechnik wird dort aber nicht betrachtet. Dabei ist die Prozessleittechnik, welche u.A. aus informationstechnischen Systemen besteht, genau der Teil, welcher erhöhte Sorgfalt durch den Betreiber benötigen würde um Versorgungsausfälle und Freisetzungen von Schadstoffen unwahrscheinlicher zu machen.

"UNBÖFI nach Störfallverordnung" ist leider nur "besser als nichts" weil es zu kurz greift. Nachhaltiger und sinnvoller wäre die Aufnahme von "Chemie" als eigener Sektor mit entsprechenden detaillierten Anlagenkategorien in der Kritis-Verordnung. In der Chemie-Branche geht es nicht nur um die Herstellung von wichtigen Grundstoffen für das produzierende Gewerbe und die Landwirtschaft, auch die Freisetzung von gefährlichen Schadstoffen im Schadensfall ist zu befürchten.

Keine Krisenreaktionspläne und keine BBK-Stärkung

Im Mai 2020 haben wir den Punkt der Krisenreaktionspläne in unserer Stellungnahme zum 2. Entwurf des ITSiG als besonders positiv hervorgehoben.

Das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) sollte im zuvor enthaltenen § 5c BSIG wichtige Aufgaben und weitere Personalstellen zugeteilt bekommen, um erstmalig in die Lage versetzt zu werden, auch für IT-Katastrophen Krisenreaktionspläne auszuarbeiten. Auch wäre der neu geschaffene § 5c BSIG fast schon wie die initiale rechtliche Grundlage für den Einsatz eines zu schaffenden Cyberhilfswerks - wie von uns im Februar 2020 vorgestellt - und verortet die Kompetenzen und Verantwortlichkeiten an den richtigen Stellen, nämlich dem BSI gemeinsam mit dem Partner BBK.

Dieser Paragraph ist leider im 3. Entwurf ersatzlos gestrichen worden - obwohl Krisenreaktionspläne als auch ein Zuwachs beim BBK dringend notwendig ist. Eine Resilienz erfordert auch die Fähigkeit auf Krisen angemessen reagieren zu können - nur mit einer Mehrausstattung von BMI und Cyber-Kräften kann diesem nicht genüge getan werden. Es erfordert zusätzliche Stellen beim BBK.

Offensive Maßnahmen gegen IT-Grundrechte

> *§ 7c Anordnungen des Bundesamtes gegenüber Diensteanbietern*
> *(1) Zur Abwehr konkreter erheblicher Gefahren für die in Absatz 2 genannten Schutzziele kann das Bundesamt gegenüber einem Anbieter von Telekommunikationsdiensten im Sinne des Telekommunikationsgesetzes (Diensteanbieter) mit mehr als 100.000 Kunden anordnen, dass er*
> *1. [...]*
> *2. technische Befehle zur Bereinigung von einem konkret benannten Schadprogramm an betroffene informationstechnische Systeme verteilt,*

Die in § 7c Abs. 1 S. 2 geplanten aktiven Maßnahmen stellen einen Eingriff in die Integrität informationstechnischer Systeme dar. Somit handelt es sich auch um einen Eingriff in das IT-Grundrecht, an den das BVerfG hohe Anforderungen stellt. Diese Anforderungen können hier nicht erfüllt werden. Darüber hinaus wird dieser Grundrechtseingriff in das IT-Grundrecht nicht einmal durch die Exekutive durchgeführt, sondern privaten Unternehmen auferlegt - so funktioniert das Gewaltmonopol nicht. Wir gehen davon aus, dass derartige Regelungen nicht verfassungskonform sein können und daher nicht wirksam werden dürfen.

Auch die Befugnisse in § 7c (3) sind rechtlich fragwürdig, da sie sehr allgemein und weitreichend formuliert sind.

> *§ 7c (3) "Ordnet das Bundesamt eine Maßnahme nach Absatz 1 Satz 1 Nummer 1 an, so kann es gegenüber dem Diensteanbieter auch anordnen, den Datenverkehr an eine vom Bundesamt benannte Anschlusskennung umzuleiten"*

Der Detailgrad von §7c Abs. S. 3 ist unzureichend. Maßnahmen, die sich aus §7c Abs. S. 3 ergeben, sind zum Beispiel Sinkholing oder Nullrouting. Diese Maßnahmen sollten explizit auf den Schutz von KRITIS oder der Zivilbevölkerung beschränkt werden und nicht zu allgemeinen Befugniserweiterung der Behörden führen. Es müssen klare Vorgaben gemacht werden, welche Art von Netzwerkverkehr (unter Wahrung von Datenschutz und Grundrechten) unter diese Maßnahmen fallen können.

Übertragung von Aufgaben der Staatsanwaltschaften auf Diensteanbieter

Änderung des TMG - § 15d Absatz 2 ff.

Bisher müssen Ermittlungsbehörden - und nur mit einem Richtervorbehalt - die Diensteanbieter anfragen um vom Betreiber die strafrechtlich benötigten Daten herausgeben zu lassen, sofern die Anfrage als berechtigt angesehen wird. Hier sollen zukünftig allerdings die Diensteanbieter eigenständig entscheiden müssen, was strafrechtlich relevant ist und dies dann

direkt an das BKA übermitteln. Ein Richtervorbehalt ist dabei nicht mehr vorgesehen und wird umgangen - die private Wirtschaft wird zum Erfüllungsgehilfen der Staatsanwaltschaften und muss Aufgaben der Rechtspflege selbst übernehmen.

Diensteanbieter werden genötigt, Teile der Entscheidung ob eine Straftat vorliegt, selbst zu treffen, proaktiv Daten zu erheben und dem Bundeskriminalamt zuzuleiten. Dies bedeutet eine Umkehr der Entscheidung über die Einleitung eines Strafverfahrens, da der Diensteanbieter nicht mehr unterstützend von der Staatsanwaltschaft und nach Beschluss eines Richters hinzugezogen wird.

Nach den bestehenden Datenschutzregelungen sind die Betreiber verpflichtet die Geschädigten bei Verlust von personenbezogenen Daten zu informieren, die im Anschluss eine Anzeige erstatten können. Die Einführung einer Meldepflicht bei den Diensteanbietern ist auch deswegen nicht nachvollziehbar, zumal Geschädigte ein Interesse haben könnten, die Strafverfolgungsbehörden nicht einbinden zu wollen.

Umgehung des Nationalen Cyber Abwehrzentrum (NCAZ)

Änderung des TMG - § 15d Absatz 1 ff.

Die vorliegende Formulierung stellt eine Umgehung des extra für diesen Fall geschaffenen "Nationalen Cyber-Abwehrzentrum" (NCAZ) im BSI dar. Im NCAZ sind alle Sicherheitsbehörden vertreten, die für die Vorfallsbehandlung zuständig sein könnten - wer wirklich zuständig ist, steht erst nach einer erfolgreichen Attributierung des Vorfalls zu einem Täter, seinem Ziel und der Nationalität des Täters fest. Nur im Fall, dass der Täter die deutsche Staatsbürgerschaft hat und zivile Diensteanbieter, Infrastruktur oder deutsche Bürger angegriffen worden sind, wäre tatsächlich das BKA zuständig - in allen anderen Fällen wären andere Sicherheitsbehörden zuständig. Zum Zeitpunkt der Feststellung einer Tatsache, die die Annahme rechtfertigt, dass eine Straftat nach § 202a ff vorliegen könnte, ist diese Attributierung jedoch noch nicht erfolgt - folgerichtig sollte der Vorfall daher im NCAZ erstbearbeitet werden.

Unterlassene Hilfeleistung: Fehlende Warnung von Betreibern

Scanning-Befugnisse des BSI zu eng gefasst

Wir begrüßen, dass das BSI zukünftig Netze untersuchen darf, um Systeme mit Sicherheitsrisiken zu identifizieren und die Betroffenen zu warnen. Die konkrete Ausgestaltung des § 7b BSIG ist aus technischer Sicht aber leider zu eng definiert.

"Detektion von Sicherheitslücken und anderen Sicherheitsrisiken an den Schnittstellen öffentlich erreichbarer informationstechnischer Systeme zu öffentlichen

Telekommunikationsnetzen" wird durch Scanmaßnahmen erreicht, die in § 7b (1) aber bereits voraussetzen, dass die Systeme als unzureichend geschützt bekannt sind. Durch dieses Kausalitätsproblem wird die Überprüfung auf Schwachstellen unnötig erschwert oder gänzlich verhindert. Daher sollten Port- und Schwachstellenscans durch das BSI grundsätzlich möglich sein.

Mit einfachen "Portscans" ohne weitergehende Interaktion mit dem gescannten System wird sich jedoch nicht überprüfen lassen, ob das System von Schwachstellen wie zum Beispiel Shitrix oder Eternal Blue betroffen ist. Daher sind zwar Portscans als erster Schritt zu begrüßen, zur Identifikation von Schwachstellen aber nicht ausreichend.

Die Einschränkung auf KRITIS, Bundessysteme und UNBÖFI sorgen dafür, dass das BSI eine Liste anlegen müsste von Systemen, die vom BSI gescannt werden dürfen. Eine solche Liste sollte jedoch nicht angelegt werden, weil diese Liste ein high-value-target für Cyberkriminelle wäre und diesen wertvolle Ziel-Informationen liefern würde.

In der Begründung ist die Argumentation zur Beschränkung auf statische IP Adressen technisch unsinnig da einerseits auch KRITIS Systeme hinter dynamischen IPv4 Adressen stecken können und andererseits in Zukunft IPv6 immer statisch ist. Weiterhin könnten auch Privatnutzer über eine Benachrichtigung durch ihre Provider profitieren.

Der Einsatz von spezialisierten (weitestgehend passiven) Suchmaschinen, wie Shodan oder Censys, wäre im vorliegenden Einsatz zum Beispiel nicht abgedeckt.

Damit ist der vorgeschlagene § 7b (1) BSIG zu eng gefasst um sein Ziel erfüllen zu können.

Unterlassung von Warnungen an KRITIS Betreiber sind intolerabel

§ 7b (3) BSIG:
Wird durch Maßnahmen gemäß Absatz 1 eine eine Sicherheitslücke oder ein anderes Sicherheitsrisiko eines informationstechnischen Systems erkannt und stehen überwiegende Sicherheitsinteressen nicht entgegen, sind die für das informationstechnische System Verantwortlichen darüber zu informieren.

Wenn konkrete Sicherheitslücken bei Systemen der Kritischen Infrastrukturen erkannt wurden, kann es keine überwiegenden Sicherheitsinteressen geben die der Benachrichtigung der für das informationstechnische System Verantwortlichen entgegenstehen. Die Betroffenen müssen immer umgehend informiert werden, damit der Betrieb der Kritischen Infrastruktur schnellstmöglich abgesichert werden kann. Dies gilt insbesondere da diese Lücken auch von Dritten in derselben Art und Weise jederzeit erkannt und ausgenutzt werden können.

Auch in § 4b (5) BSIG wird für gemeldete oder bekannt gewordene Informationen zu Sicherheitslücken, Schadprogrammen, erfolgten oder versuchten Angriffen die Meldung nach §

8b Absatz 2 Nummer 4 Buchstabe a) an Betreiber Kritischer Infrastrukturen potenziell aufgrund von sonstigen "Übermittlungshindernissen" unterschlagen. Informationen zu Schwachstellen müssen konsequent zur Behebung derselben und zur Absicherung von Systemen genutzt werden und dürfen nicht zur Schwächung der IT-Sicherheit zurückgehalten oder z.B. für die Entwicklung von Staatstrojanern an andere Stellen wie Sicherheitsbehörden oder Geheimdienste weitergegeben werden.

Vertrauenswürdige Hersteller - Lex Huawei für KRITIS?

§ 9b (5) S. 3 (et al.)

Der § 9b ist in seiner Ausprägung nicht sinnvoll: Wesentliche Aspekte sind unvollständig oder hinsichtlich ihres Zwecks unklar. Eigentlich müsste man diesen Abschnitt "Lex Huawei" nennen, da offensichtlich ist, dass es hier um die juristische Möglichkeit des Ausschlusses bestimmter Hersteller geht. Auch wenn es im Mobilfunk- und Kommunikationsbereich durchaus auch andere Hersteller gibt, so ist das nicht in allen Sektoren der Fall. Resilienz darf nicht auf dem Verbot einzelner Hersteller basieren, sondern Betreiber und Hersteller müssen aktiv dabei unterstützt werden Resilienz zu fördern und zu realisieren.

Wir begrüßen grundsätzlich, dass Hersteller von Software für Kritische Infrastruktur und Betreiber Kritischer Infrastrukturen selbst an einer Sicherheitsüberprüfung (bspw. Penetrationstest) mitwirken müssen - dies kann zu einem hohen Maß an Sicherheit und Transparenz führen. Nichtsdestotrotz erscheint die Norm insgesamt aber problematisch und zweifelhaft, z.B. weil die Komponenten nicht direkt vom Hersteller an die Betreiber verkauft werden, sondern im Rahmen einer Wertschöpfungskette - an der Reseller und Systemhäuser und andere Unternehmen teilnehmen - in Kritische Infrastrukturen verbaut werden. Viele Lieferanten wissen nicht (bzw. können gar nicht wissen) in welchen Infrastrukturen ihre Produkte eingesetzt werden - die Pflicht den Betreiber nach Satz 4 zu warnen kann daher gar nicht nachgekommen werden.

Hinzu kommt dass es Kritische Komponenten gar nicht geben sollte (siehe Abschnitt "Resilienz kommt zu kurz"). Die Maßnahmen im § 9b sind für den Schutz Kritischer Infrastrukturen schlichtweg nicht zielführend.

Auf eine Option zum Umgang mit Herstellern, die ein Quasimonopol in einzelnen Sektoren haben, wird im vorliegenden Entwurf nicht eingegangen. Gleiches gilt für die Berücksichtigung von Lieferketten und zuliefernden Herstellern.

Es muss sichergestellt werden, dass Transparenz und Kooperation von Herstellern hinsichtlich des Umgangs mit Sicherheitsschwachstellen, nicht zu einer Schlechterstellung gegenüber Mitbewerbern oder gar der Untersagung des Einsatzes führen dürfen. Die Möglichkeit, dass die

eigenen Produkte in der Folge einer ordnungsgemäßen Meldung einer Schwachstelle vom Einsatz ausgeschlossen werden können wird dazu führen, das Hersteller Schwachstellen trotz gesetzlicher Verpflichtung eher nicht melden werden. Dieses Gesetz setzt so also falsche Anreize.

Die vollständige Untersagung nach Absatz 7 kann in dieser Pauschalität nicht zielführend sein - Fehler passieren, und Hersteller müssen die Chance haben, andere Produkte als die zuvor vom BMI bemängelten, weiterhin am Markt verkaufen zu können - wenn die IT-Sicherheit dieser Produkte nicht zu bemängeln ist.

Auch umgeht diese Regelung das Prinzip der Schutzbedarfsfeststellung und Risikoanalyse - Systeme die z.B. an keine Datennetze angebunden sind müssen auch nicht zwingend in der vom § 9b beschriebenen Variante geprüft werden. Die Entscheidung welche Risiken und Gefahren vom Einsatz eines Systems ausgehen hängt maßgeblich von der Art und Weise der Integration in die Infrastruktur ab und der verarbeiteten Daten.

Resilienz kommt zu kurz: Kritische Infrastruktur vs. Kritische Komponenten

Die Begründung zur Einführung des Begriffs Kritische Komponenten zeigt, dass ein wesentlicher Aspekt des Schutzes Kritischer Infrastrukturen nicht berücksichtigt wurde. Das Zusammenspiel aller relevanten Komponenten in der Architektur ist Wesentlich für die Versorgung, nicht einzelne Komponenten. Da die IT-technische Architektur aber bereits die Anforderungen zur Gewährleistung einer zuverlässigen Versorgung erfüllen muss, bedarf es dieser besonders kontrollierten Kritischen Komponenten aus technischer Sicht nicht.

Gerade der aktualisierte Formulierungsvorschlag des § 2 (13) BSIG aus dem zweiten zum dritten Referentenentwurf legt eine rein politische Motivation nahe. Wo im Mai 2020 noch vorgesehen war, dass das BSI die Liste Kritischer Komponenten aus fachlichen und abgestimmten Erwägungen heraus festlegt, so steht jetzt nur noch lapidar "Alle übrigen kritischen Komponenten werden gesetzlich festgelegt". Eine tatsächliche Verbesserung der Resilienz oder der Versorgungssicherheit ist nicht erkennbar.

Keine Änderung an Strafprozessordnung und am Strafgesetzbuch

Die Abschnitte zur Strafprozessordnung und am Strafgesetzbuch, welche in einem früheren Entwurf enthalten waren, sind in diesem Entwurf nicht mehr enthalten, was wir begrüßen.

Herausgabe von Informationen zur Bewältigung einer erheblichen Störung

Seite 16 - Änderung von § 8b Absatz 4a

Es ist nicht nachvollziehbar, warum im Fall einer erheblichen Störung das BSI zur Herausgabe von Informationen das Einvernehmen mit der für den jeweiligen Betreiber zuständigen Aufsichtsbehörde suchen muss - die Bewältigung der Störung muss Priorität über die Befindlichkeiten der zuständigen Aufsichtsbehörde haben. Unserer Ansicht nach würde es vollkommen ausreichen, die zuständige Aufsichtsbehörde in Kenntnis zu setzen. Dieses Detail halten wir für einen groben handwerklichen Fehler, der die Bewältigung einer erheblichen Störung unnötig verzögert.

KRITIS bekommt Zähne: erhöhte BSI Bußgelder

§ 14 Abs. 2 BSIG

Grundsätzlich begrüßen wir, dass die BSI Bußgeldstelle nun durch die Erhöhung des Bußgeldberechnungsrahmen Zähne bekommt und Kritische Infrastrukturen ernst genommen werden. Die Höhe von maximal 2 Mio. € in Verbindung mit dem § 30 Absatz 2 Satz 3 des Ordnungswidrigkeitengesetz (OWiG) beträgt dann für juristische Personen 20 Mio. € - also die gleiche Summe, die auch in der DSGVO vorgesehen ist.

Dies drängt die Frage auf: Sind Kritische Infrastrukturen genau so wichtig wie das Recht auf informationelle Selbstbestimmung und der Datenschutz der Bürger, oder sind Kritische Infrastrukturen wichtiger?

Die bisher fehlende Evaluierung des IT-Sicherheitsgesetz hätte die Möglichkeit geboten, sich nicht nur unkreativ an der DSGVO zu orientieren, sondern auf Basis von tatsächlicher Evidenz einen Bußgeldrahmen festzulegen, der von KRITIS-Betreibern nicht einfach eingepreist werden kann und tatsächlich wirksam ist.

Deutscher Alleingang: IT-Sicherheitskennzeichen

Die Regelungen des § 9c sind im Kern deckungsgleich mit den in § 9a geregelten Sachverhalten. Genau diese Aufgabe übernimmt bereits der § 9a. Um unnötige Doppelstrukturen und deutsche Alleingänge zu verhindern, muss der § 9c BSIG ersatzlos gestrichen werden. Die Umsetzung des EU Cyber Security Acts (CSA) behandelt bereits notwendige Aspekte zu Zertifizierungen - diese können sich auch auf Consumer Devices erstrecken - daher empfehlen wir die Bindung von Personal (Ressourcen) durch den § 9c zu verhindern und sind der Überzeugung, dass wir diese Themen gesamteuropäisch regeln müssen.

Vorherige Stellungnahme der AG KRITIS

https://ag.kritis.info/2020/05/13/kommentar-zum-neuen-referentenentwurf-des-it-sicherheitsgesetz-2-0-it-sig2/

Bei weiteren sachdienlichen Hinweisen wenden Sie sich bitte an Ihre nächste Kontaktperson der AG KRITIS.

Für Risiken und Nebenwirkungen kontaktieren Sie Ihre Abgeordneten im deutschen Bundestag und Ihren Bundesminister für Heimat, Bau und Inneres.

Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Prof. Ulrich Kelber
Bundesbeauftragter
für den Datenschutz und
die Informationsfreiheit

POSTANSCHRIFT Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
Postfach 1468, 53004 Bonn

Deutscher Bundestag
Ausschuss für Inneres und Heimat
Platz der Republik 1

Per Email an
innenausschuss@bundestag.de

HAUSANSCHRIFT Graurheindorfer Straße 153, 53117 Bonn

FON (0228) 997799-5000
FAX (0228) 997799-5550

E-MAIL referat23@bfdi.bund.de

INTERNET www.bfdi.bund.de

DATUM Bonn, 18.12.2020
GESCHÄFTSZ. 23-170/024#0877

Bitte geben Sie das vorstehende Geschäftszeichen bei allen Antwortschreiben unbedingt an.

BETREFF **Gesetzentwurf eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme**

Sehr geehrte Frau Ausschussvorsitzende Lindholz,
sehr geehrte Damen und Herren,

der vom Bundesminister des Innern, für Bau und Heimat vorgelegte Entwurf eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme wurde von der Bundesregierung in der Kabinettsitzung am 16. Dezember 2020 beschlossen.

Anliegend übersende ich Ihnen meine korrespondierende Stellungnahme verbunden mit der Bitte um freundliche Berücksichtigung.

Mit besten Grüßen

[redacted]
Ulrich Kelber

ZUSTELL- UND LIEFERANSCHRIFT Graurheindorfer Straße 153, 53117 Bonn
VERKEHRSANBINDUNG Straßenbahn 61 und 65, Innenministerium
Bus 550 und SB60, Innenministerium

Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Bonn, den 18.12.2020

Stellungnahme

des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

zum Entwurf eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0)

Graurheindorfer Str. 153
53117 Bonn
FON +49 (0)228-997799-0
FAX +49 (0)228-997799-5550
E-MAIL poststelle@bfdi.bund.de
INTERNET www.bfdi.bund.de

Cyber- und Informationssicherheit ist wichtiger Vertrauensanker

Die Digitalisierung durchdringt alle Lebensbereiche. Die Cyber- und Informationssicherheit ist hierbei ein essentieller Vertrauensanker. Digitalisierung, Cybersicherheit und Datenschutz sind untrennbar miteinander verbunden. IT-Sicherheitsvorfälle bedrohen regelmäßig auch die Schutzgüter des Datenschutzes. Das mit der Novelle des IT-Sicherheitsgesetzes verfolgte Ziel eines verbesserten Schutzes von Gesellschaft und Wirtschaft in der digitalen Welt unterstütze ich deshalb nachdrücklich. Hierauf gerichtete Maßnahmen müssen aber in Einklang mit dem Datenschutz stehen.

Das IT-Sicherheitsgesetz 2.0 wird bereits seit geraumer Zeit diskutiert. Ein erster Gesetzentwurf wurde mir bereits im Frühjahr 2019 auf Ressortebene zugeleitet. Ein zweiter Entwurf folgte im Mai 2020. Der dritte Referentenentwurf wurde im November 2020 zirkuliert. Trotz dieses langen Zeitraums waren die Fristen für meine Stellungnahmen stets äußerst ambitioniert bemessen. Im Rahmen dieser schwierigen Bedingungen wurde das Verfahren bestmöglich begleitet. Es fand ein intensiver Austausch auf Ressortebene statt. Viele meiner Kritikpunkte wurden hierbei aufgegriffen und umgesetzt. Diverse ursprünglich geplante, aus meiner Sicht überbordende und deshalb datenschutzrechtlich kritische Neuregelungen u.a. im Straf- und Strafprozessrecht wurden gestrichen, was ich sehr begrüße.

Keine unangemessene Ausweitung der Speicherdauer von Protokolldaten

Weiterhin kritisch sehe ich aber insbesondere die in dem Gesetzentwurf in Artikel 1 Nr. 4, § 5 Abs. 2 BSIG-Entwurf (Gesetz über das Bundesamt für Sicherheit in der Informationstechnik) geplante Ausweitung der Speicherung von Protokolldaten von bisher drei auf zwölf Monate.

Meine zugrundeliegenden Bedenken basieren auf folgenden Überlegungen:

Im Gesetzentwurf wird damit argumentiert, diese Ausweitung sei für eine effektive Aufklärung von Cyberangriffen unerlässlich. Denn Cyberangriffe würden sich typischerweise über einen längeren Zeitraum erstrecken und nur mit vorhandenen Protokolldaten sei eine Rekonstruktion des Angriffs und eine bestmögliche Schadensbeseitigung möglich. Die Motivation für die längere Speicherdauer ist nachvollziehbar, rechtfertigt aus meiner Sicht aber nicht ihre erhebliche Ausweitung und wirft Fragen der Verhältnismäßigkeit auf.

Die Speicherung von Protokolldaten für zwölf Monate wird die Regel und nicht die Ausnahme sein. Eine Speicherung von Protokolldaten darf nach dem BSIG bereits heute erfolgen, wenn tatsächliche Anhaltspunkte bestehen, dass die Protokolldaten zur Abwehr einer bereits bestehenden Gefahr erforderlich sein können. Konkret müssen der Norm entsprechend tatsächliche Anhaltspunkte bestehen, „dass diese [Protokolldaten] für den Fall der Bestätigung eines Verdachts nach Absatz 3 Satz 2 [BSIG] zur Abwehr von Gefahren, die von dem gefundenen Schadprogramm ausgehen oder zur Erkennung und Abwehr anderer Schadprogramme erforderlich sein können“. Diese Voraussetzung dürfte stets anzuneh-

men sein, so dass eine Speicherung der Protokolldaten nicht nur Ausnahmecharakter haben dürfte.

Nach der gesetzlichen Definition von Protokolldaten in § 2 Abs. 8 S. 2 BSIG können Protokolldaten Verkehrsdaten enthalten, so dass es sich insoweit um eine „Vorratsdatenspeicherung“ handelt. Eine unterschiedslose Speicherung ohne konkreten Anlass stellt einen besonders schwerwiegenden Eingriff in die Grundrechte der Betroffenen dar, weil kein Zusammenhang zwischen dem Verhalten der Personen, deren Daten betroffen sind, und dem mit der fraglichen Regelung verfolgten Zweck vorliegt.

Generell gilt, dass die Speicherdauer von Protokolldaten auf das zwingend notwendige Maß zu beschränken ist. Das Bundesverfassungsgericht führte hierzu bereits vor einer Dekade in einem Grundsatzurteil zur konkreten Ausgestaltung der Vorratsdatenspeicherung aus, dass eine Speicherungsdauer von sechs Monaten „an der Obergrenze dessen [ist], was unter Verhältnismäßigkeitserwägungen rechtfertigungsfähig ist“, vgl. BVerfG, Urteil des Ersten Senats vom 02. März 2010 - 1 BvR 256/08 -, Rn. 215. Bereits in diesem Lichte begegnet die geplante Ausweitung der Speicherdauer erheblichen rechtlichen Bedenken mit Blick auf ihre Verhältnismäßigkeit.

Die Ausweitung der Speicherdauer zur Stärkung der Cyber-Resilienz der Kommunikationstechnik des Bundes würde zusätzlich aber auch die - bereits heute bestehende - Inkongruenz zum privatwirtschaftlichen Telekommunikationssektor weiter vergrößern. In der Telekommunikationsbranche können Verkehrsdaten z.B. für die Störungserkennung, dem Schutz vor Missbrauch und für die generelle Netzsicherheit genutzt werden, vgl. § 100 Abs. 1 und 3 und § 109 Telekommunikationsgesetz. Hier werde ich (sofern kein konkreter Anlass besteht, etwa eine konkrete Störung) auch weiterhin auf eine maximale Speicherdauer von sieben Tagen bestehen.

Die geplante Ausweitung der Speicherdauer in § 5 Abs. 2 BSIG-Entwurf ist nach alledem abzulehnen.

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
19(4)714

FACHBEREICH
SICHERHEIT – SCHUTZ
UND ZUVERLÄSSIGKEIT

Berlin, 9. Dezember 2020

Stellungnahme

des Fachbereichs Sicherheit – Schutz und Zuverlässigkeit – der Gesellschaft für Informatik e.V.

zum Entwurf eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (Zweites IT-Sicherheitsgesetz – IT-SiG 2.0)

des Bundesministeriums des Innern, für Bau und Heimat (BMI)

Ansprechpartner und Autor:
Bernhard C. Witt, Sprecher des GI-Fachbereichs „SICHERHEIT“, bcwitt@it-sec.de

Einleitung

Durch Veröffentlichung des Entwurfs eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (Zweites IT-Sicherheitsgesetz – IT-SiG 2.0) zum 02.12.2020 auf https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/entwurf-zweites-it-sicherheitsgesetz.html wurde seitens des Bundesministeriums des Inneren, für Bau und Heimat dazu aufgerufen, Stellungnahmen bis zum 09.12.2020 per Mail an CI1@bmi.bund.de einzureichen.
Der Fachbereich Sicherheit – Schutz und Zuverlässigkeit – der Gesellschaft für Informatik e.V. nimmt diese Gelegenheit gerne wahr und nimmt zu dem Gesetzesentwurf vor allem zu Artikel 1, der die Änderung des bestehenden BSIG umfasst (im Folgenden daher als BSIG-E referenziert), Stellung. Die Stellungnahme erfolgt unter Berücksichtigung vorausgehender Beiträge folgender GI-Gremien:

- Präsidiumsarbeitskreis Datenschutz und IT-Sicherheit der GI, dieser Stellungnahme als Anlage beigefügt (https://gi.de/fileadmin/GI/Allgemein/PDF/2020-12-02_GI_PAK_IT-SiG_20_FINAL.pdf)
- GI-Fachgruppe Ada – Zuverlässige Software-Systeme, dieser Stellungnahme als Anlage beigefügt (https://gi.de/fileadmin/GI/Allgemein/PDF/2019-05-22_Stellungnahme_IT_Sicherheitsgesetz.pdf)
- GI-Fachgruppe Datenschutzfördernde Technik

Zu § 2 Abs. 14 BSIG-E: Unternehmen im besonderen öffentlichen Interesse

Insgesamt wird die Erweiterung der KRITIS-Verpflichteten begrüßt. Die Einbeziehung der größten Unternehmen gemäß ihres Wertschöpfungsbeitrags erscheint dagegen recht unspezifisch zu sein, im Hinblick darauf, dass es um den Schutz kritischer Infrastrukturen geht. Zielführender wäre es aus Sicht des GI-Fachbereichs Sicherheit, Zulieferer und Hersteller darunter einzuordnen, die innerhalb eines Sektors eine maßgebliche Bedeutung haben, d.h. mind. 50 % der im Sektor gelisteten kritischen Infrastrukturen mit Schlüsseltechnik bedienen. Das ist z.B. bei der Leittechnik so für Energie & Wasser - diese fallen aber nicht notwendigerweise unter die Wertschöpfungsdefinition. Dies könnte zugleich ein wertvoller Beitrag zur digitalen Souveränität darstellen.

Zu § 3 Abs. 1 Nr. 20 BSIG-E: Aufgabe des BSI im Kontext Stand der Technik

Gemäß Gesetzentwurf soll das Bundesamt für Sicherheit in der Informationstechnik die Aufgabe zugewiesen bekommen, einen Stand der Technik bei sicherheitstechnischen Anforderungen an IT-Produkte zu entwickeln und zu veröffentlichen. Diese Aufgabe ist aus mehreren Gründen missverständlich:

1. Stand der Technik ist laut Gesetzesbegründung des bestehenden Gesetzes wie folgt definiert worden (siehe Drucksache 18/4096, S. 26): „Stand der Technik in diesem Sinne ist der Entwicklungsstand fortschrittlicher Verfahren, Einrichtungen oder Betriebsweisen, der die praktische Eignung einer Maßnahme zum Schutz der Funktionsfähigkeit von informationstechnischen Systemen, Komponenten oder Prozessen gegen Beeinträchtigungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit gesichert erscheinen

lässt." Damit ist bereits festgelegt, was als Stand der Technik zu verstehen ist. Aus Sicht des GI-Fachbereichs Sicherheit zeigt jedoch der vorliegende Gesetzesentwurf, dass es zweckmäßig wäre, diese Definition als Legaldefinition in das BSIG ausdrücklich in § 2 als neuer Abs. 15 aufzunehmen.

2. Das BSI kann in diesem Sinne folglich keinen Entwicklungsstand entwickeln, denn dieser resultiert aus unternehmerischer und wissenschaftlicher Forschung und Entwicklung und hängt insbesondere im Einklang mit den weiteren Ausführungen aus der damaligen Gesetzesbegründung davon ab, was einschlägige internationale, europäische und nationale Normen und Standards ausweisen und welche Verfahren, Einrichtungen und Betriebsweisen mit Erfolg in der Praxis erprobt wurden. Insoweit kann es aus Sicht des GI-Fachbereichs Sicherheit allenfalls Aufgabe des BSI sein, diesen Stand der Technik zu beschreiben, nicht aber diesen zu entwickeln.

Zu § 7b, 8f, 9a und 9c BSIG-E: Neue Befugnisse des BSI

Im Zuge des Gesetzesentwurfs soll das Bundesamt für Sicherheit in der Informationstechnik weitreichende, neue Befugnisse erhalten: Es soll demnach

- Sicherheitsrisiken detektieren dürfen nach § 7b BSIG-E,
- in begrenztem Umfang Aufsichtsfunktionen übernehmen über Unternehmen im besonderen öffentlichen Interesse nach § 8f BSIG-E, die zumindest nach aktuellem Stand des Gesetzesentwurfs Unternehmen in Abhängigkeit ihres Wertschöpfungsbeitrags umfassen,
- die Cybersicherheitszertifizierung durchführen nach § 9a BSIG-E und
- Aufgaben zum digitalen Verbraucherschutz im Kontext des freiwilligen IT-Sicherheitskennzeichens erhalten.

Aus Sicht des GI-Fachbereichs Sicherheit sind das allesamt Aufgaben, die einer Beibehaltung der Zuordnung des BSI an das BMI entgegenstehen und es erfordern, dass das BSI als eigenständige oberste Bundesbehörde, vergleichbar zum Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, konstitutionell neu aufgestellt wird. Insoweit wird durch den GI-Fachbereich Sicherheit nachdrücklich eine entsprechende Änderung des § 1 BSIG empfohlen.

Zu § 7b BSIG-E: Detektion von Sicherheitsrisiken für die Netz- und IT-Sicherheit

Oberstes Schutzziel im Rahmen von KRITIS ist bereits nach bestehendem § 8a BSIG die Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der informationstechnischen Systeme, Komponenten oder Prozesse, die für die Funktionsfähigkeit der betriebenen Kritischen Infrastrukturen maßgeblich sind. Aus Sicht des GI-Fachbereichs Sicherheit ist es daher zwingend erforderlich, dass durch die vom BSI selbst oder im Auftrag durchgeführten Portscans und vergleichbaren Tests die Funktionstüchtigkeit der kritischen Dienstleistung nicht gefährdet werden darf, was damit als ergänzendes Kriterium in § 7b BSIG-E aufzunehmen ist. Weitere Ausführungen hierzu, auch zur Notwendigkeit der Veröffentlichung von entsprechenden Erkenntnissen, sind in der beigefügten

Stellungnahme des GI-Präsidiumsarbeitskreises Datenschutz und IT-Sicherheit ausgeführt.

Zu § 8a Abs. 1b BSIG-E: Aufbewahrungspflicht von Daten zur Angriffserkennung und -nachverfolgung

Betreiber einer kritischen Infrastruktur sollen gemäß dem Gesetzentwurf 4 Jahre lang Daten zur Angriffserkennung und -nachverfolgung vorhalten. Das BSI selbst, welches entsprechende Daten auswertet, ist jedoch angehalten, diese nach § 5 Abs. 2 BSIG-E nur 1 Jahr lang zu speichern. Aus Sicht des GI-Fachbereichs Sicherheit ist die Frist für die Betreiber einer kritischen Infrastruktur damit ebenfalls auf 1 Jahr zu begrenzen, da längere Speicherfristen offensichtlich unnötig und damit unverhältnismäßig sind.

Zu § 9b BSIG-E: Untersagung des Einsatzes kritischer Komponenten

Neu aufgenommen werden soll eine an sich durchaus effektive Befugnis, den Einsatz kritischer Komponenten zu untersagen. Aus Sicht des GI-Fachbereichs Sicherheit fehlt es hier bisher angesichts des damit verbundenen sehr weitgehenden Eingriffes in Eigentumsrechte der Betreiber einer kritischen Infrastruktur einer präzisen rechtswirksamen Festlegung und einer ausreichend langen Übergangsfrist, zumal es sich im Kontext von kritischen Infrastrukturen hierbei überwiegend um solche Komponenten handeln dürfte, die über einen längerfristigen LifeCycle verfügen und die gesamte Zertifizierungslandschaft überhaupt erst noch aufgebaut werden muss. Eine derart weitreichende Kompetenz setzt zudem aus Sicht des GI-Fachbereichs Sicherheit voraus, dass damit eine ausreichende Gewaltenteilung sichergestellt ist, die zulassende und prüfende Kompetenzen differenziert, wie in der beigefügten Stellungnahme der GI-Fachgruppe Ada näher ausgeführt. Andernfalls zweifelt der GI-Fachbereich Sicherheit an der Verfassungsmäßigkeit einer solchen Regelung.

Ergänzende Empfehlungen:

Aus Sicht des GI-Fachbereichs Sicherheit wären neben den oben bereits aufgeführten Anpassungen in den §§ 1 und 2 BSIG folgende Regelungen mitaufzunehmen:

- Kritische Infrastrukturen sollten ausdrücklich gesetzlich dazu verpflichtet werden, einen ausreichend unabhängigen Informationssicherheitsbeauftragten (analog zur Funktion eines Datenschutzbeauftragten) zu benennen
- Die Bundesländer sollten dazu verpflichtet werden, näher zu verfolgen, welche kritischen Infrastrukturen auf ihrem Landesgebiet angesiedelt sind, weshalb das BSI zugleich über eine entsprechende Übermittlungsbefugnis von entsprechenden Registrierungsdaten verfügen sollte

Anlagen:

- Stellungnahme des Präsidiums-Arbeitskreises „Datenschutz und IT-Sicherheit“ der Gesellschaft für Informatik e.V. (GI) zum dritten Referentenentwurf eines

Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0 –IT-SiG 2.0) des Bundesministeriums des Innern, für Bau und Heimat (BMI) vom 02.12.2020

- Stellungnahme der Fachgruppe ADA – Zuverlässige Software-Systeme der Gesellschaft für Informatik e.V. zum Entwurf des Bundesministeriums des Innern, für Bau und Heimat für ein „IT-Sicherheitsgesetz 2.0“ vom 21.05.2019

Über den Fachbereich Sicherheit – Schutz und Zuverlässigkeit – der Gesellschaft für Informatik e.V.

Der GI-Fachbereich "Sicherheit -Schutz und Zuverlässigkeit" wurde im Februar 2002 gegründet und vernetzt zwei "Communities" miteinander: Während die „Safety-Community“ vor allem den Schutz der Umwelt vor IT-Systemen (beispielsweise Sicherheit des Menschen vor schwerwiegenden Systemfehlern in Flugzeugen, Kernreaktoren und Kraftwerken) sowie Fehlertoleranzmaßnahmen (z.B. Systemausfälle als Folge von Ermüdungserscheinungen, Softwarefehlern und Naturereignissen) im Blick hat, beschäftigt sich die „Security-Community“ hauptsächlich mit dem Schutz der IT-Systeme und ihrer Umgebung vor Bedrohungen von außen, insbesondere vor Gefahren, die von bösartigen Angriffen (durch Menschen) ausgehen. Der Fachbereich bietet ein Forum, in dem alle auf dem Gebiet der Sicherheit informationstechnischer Systeme arbeitenden Menschen ihr Fachthema, organisiert in Fachgruppen, wiederfinden. Neben der rein wissenschaftlichen Arbeit ermöglicht der Fachbereich einen fachlichen Austausch zwischen Wissenschaft und Praxis. Mehr Information über den Fachbereich Sicherheit der GI kann der Webseite https://fb-sicherheit.gi.de/ entnommen werden.

Über die Gesellschaft für Informatik e.V.

Die Gesellschaft für Informatik e.V. (GI) ist mit rund 20.000 persönlichen und 250 korporativen Mitgliedern die größte und wichtigste Fachgesellschaft für Informatik im deutschsprachigen Raum und vertritt seit 1969 die Interessen der Informatikerinnen und Informatiker in Wissenschaft, Wirtschaft, öffentlicher Verwaltung, Gesellschaft und Politik. Mit 14 Fachbereichen, über 30 aktiven Regionalgruppen und unzähligen Fachgruppen ist die GI Plattform und Sprachrohr für alle Disziplinen in der Informatik. Weitere Informationen finden Sie unter www.gi.de.

Die GI-Mitglieder binden sich an die Ethischen Leitlinien für Informatikerinnen und Informatiker der Gesellschaft für Informatik e.V.: https://gi.de/ethische-leitlinien

AOK Die Gesundheitskasse. | BUNDESVERBAND

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
19(4)721

Stellungnahme des

AOK-Bundesverbandes

zum

Entwurf eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme

Bundestags-Drucksache 19/26106

Stand 04.02.2021

AOK-Bundesverband
Rosenthaler Straße 31
10178 Berlin

Tel. 030/ 3 46 46 - 2299

Inhaltsverzeichnis:

I. Zusammenfassung ..... - 3 -

II. Stellungnahme zu einzelnen Regelungen des Gesetzentwurfs ..... - 4 -

Artikel 1 Änderung des BSI-Gesetzes ..... - 4 -

§ 7b Detektion von Sicherheitsrisiken für die Netz- und IT-Sicherheit und von Angriffsmethoden ..... - 4 -

§ 8a Anschaffung von Systemen zur Angriffserkennung ..... - 5 -

§ 9b Untersagung des Einsatzes kritischer Komponenten..... - 6 -

I. Zusammenfassung

Es ist zu begrüßen, dass mit diesem Gesetzentwurf die sicherheitstechnischen IT-Fortschritte und die damit verbundenen Risiken aufgegriffen werden.

Anzuerkennen ist, dass die Anregungen der betroffenen Betreiber kritischer Infrastrukturen und Unternehmen im öffentlichen Interesse im Rahmen der Verbändebeteiligung zum Referentenentwurf in wesentlichen Punkten in diesem Gesetzentwurf aufgegriffen wurden. Gleichwohl bestehen weiterhin wirtschaftliche und betriebliche Risiken für die Betreiber kritischer Infrastrukturen durch fehlende Konkretisierungen, ambitioniert gefasste Befugnisse und Vorlaufzeiten in den vorgesehenen Regelungen.

II. Stellungnahme zu einzelnen Regelungen des Gesetzentwurfs

Artikel 1 Änderung des BSI-Gesetzes

§ 7b Detektion von Sicherheitsrisiken für die Netz- und IT-Sicherheit und von Angriffsmethoden

A Beabsichtigte Neuregelung

Die ergänzende Regelung in Absatz 1 eröffnet dem Bundesamt die Möglichkeit, sogenannte Portscans zur Ermittlung von Sicherheitslücken und anderen Sicherheitsrisiken in der Informationstechnik bei dem Bund, den Betreibern kritischer Infrastrukturen sowie Unternehmen im besonderen öffentlichen Interesse auch ohne Kenntnis der jeweiligen Betreiber durchzuführen.

B Stellungnahme

Es ist anzunehmen, dass mit der Durchführung von Portscans Schwachstellen bei Betreibern kritischer Infrastrukturen ermittelt werden sollen.

Der Nutzen dieses Vorgehens ist jedoch zweifelhaft und bindet in der beschriebenen Form zusätzliche Ressourcen bei den Betreibern, da die Netzwerkaktivitäten ohne vorherige Abstimmung als Angriffsversuch interpretiert werden könnten.

Die bloße Ermittlung von potenziell risikobehafteten Ports lässt darüber hinaus keine verlässliche Auskunft über die dahinterliegende Anwendung zu und kann somit auch nicht zuverlässig einer Sicherheitslücke und oder einem anderen Sicherheitsrisiko zugeordnet werden. Ein systematisches Vorgehen zur Ermittlung von Risiken ist daher in Abstimmung mit den Betreibern, bei denen die Durchführung von Portscans erfolgen soll, zu bevorzugen.

C Änderungsvorschlag

Einfügen des nachfolgenden Satz nach Satz 4 im Absatz 1:

„Maßnahmen nach Satz 1 dürfen nur im Einvernehmen mit den jeweiligen Betreibern kritischer Infrastrukturen oder Unternehmen im besonderen öffentlichen Interesse durchgeführt werden.“

§ 8a Anschaffung von Systemen zur Angriffserkennung

A Beabsichtigte Neuregelung

Betreiber Kritischer Infrastrukturen müssen Systeme zur Angriffserkennung nach dem vom Bundesamt festgelegten Standards vorhalten.

B Stellungnahme

Je nach Größe des Betreibers bzw. Netzwerkdurchsatzes kann die geplante Regelung zu regelmäßigen erheblichen Investitionen und Betriebsaufwänden führen. Die hierfür erforderlichen Aufwände müssen daher durch Mittel des Bundes gegenfinanziert werden.

Gleichzeitig bedarf die Verpflichtung der KRITIS-Betreiber zur Anschaffung von Produkten für die Angriffserkennung einer deutlichen und präzisen Definition der erforderlichen Mindestfunktionen sowie die realistische Verfügbarkeit solcher Produkte am Markt.

Die Regelung zur Speicherung von Daten über einen Zeitraum von vier Jahren muss präzisiert werden. Es ist unklar, ob der Gesetzgeber für Protokollierungsdaten vier Jahre vorsieht. Falls dies der Fall ist, sind Aufwand und Kosten für die Speicherung erheblich, ohne dass diese anonymisierten Daten nach vier Jahren noch einen besonderen Nutzen für die Ziele der Gesetzgebung und der IT-Sicherheit darstellen. Eine Speicherdauer von maximal einem Jahr wäre angemessen.

C Änderungsvorschlag

§ 8a Abs. 1b wird wie folgt geändert:

„Betreiber Kritischer Infrastrukturen müssen für die Angriffserkennung und Angriffsnachverfolgung relevante, nicht personenbezogene Daten, die beim Betrieb einer Kritischen Infrastruktur anfallen, mindestens ein Jahr speichern.“

§ 9b Untersagung des Einsatzes kritischer Komponenten

A Beabsichtigte Neuregelung

Es wird eine Anzeigepflicht gegenüber dem Bundesministerium des Innern, Bau und Heimat für kritische Komponenten eingeführt. Der Betrieb von kritischen Komponenten kann durch die Behörde untersagt werden.

B Stellungnahme

Bei einer Untersagung des Einsatzes von kritischen Komponenten, die vom Betreiber nicht vorhersehbar waren, müssen die hierfür erforderlichen Aufwände durch Mittel des Bundes gegenfinanziert werden. Es muss sichergestellt sein, dass getätigte Investitionen der KRITIS-Betreiber geschützt werden. Eine nachträgliche Untersagung von eingesetzten Komponenten führt zu unverhältnismäßigen wirtschaftlichen und betrieblichen Risiken.

Die geforderten Fristen sind in der Praxis unverhältnismäßig und müssen unter Berücksichtigung der Schutzziele der Informationssicherheit gegenüber Schadensausmaß abgewogen werden. Die Untersagung des Einsatzes von kritischen Komponenten muss das Risiko in der jeweiligen Betriebsumgebung berücksichtigen.

C Änderungsvorschlag

Streichung des 2. Satzes im Absatz 3 und Anfügen der folgenden Sätze nach Satz 1:

„Die Frist zum Weiterbetrieb der kritischen Komponente ist im Einvernehmen mit dem jeweiligen Betreiber unter Berücksichtigung des Risikos für die öffentlichen Interessen festzulegen.

Wird die Untersagung einer in Betrieb befindlichen kritischen Komponente angeordnet, müssen die Kosten durch Mittel des Bundes gegenfinanziert werden.“

Deutscher Bundestag

Ausschuss für Inneres und Heimat

Ausschussdrucksache
19(4)726

VDV Die Verkehrsunternehmen

VDV | GFT, KB, T21

Köln, Berlin | 18. Jan. 2021

Stellungnahme zum Entwurf eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0)

Der Verband Deutscher Verkehrsunternehmen (VDV), Branchenverband für über 600 Unternehmen des Öffentlichen Personen- und Schienengüterverkehrs in Deutschland, begrüßt grundsätzlich die Weiterentwicklung des Ordnungsrahmens zum Schutz informationstechnischer Systeme von Kritischen Infrastrukturen. Denn auch die Anlagen und Einrichtungen sowie technischen Systeme im Nah- und Fernverkehr gehören zu den „Kritischen Infrastrukturen" (KRITIS) und sind für die Sicherung der Mobilitätsangebote von zentraler Bedeutung. Das betrifft nicht nur den Öffentlichen Personennahverkehr (ÖPNV) als Teil der Daseinsvorsorge, der Versorgungsmöglichkeiten und die gesellschaftliche Teilhabe aller Menschen absichert, sondern auch den Güterverkehr auf der Schiene. Insbesondere zu Beginn der Corona-Pandemie, als viele Grenzübergänge auf den Autobahnen vorübergehend geschlossen worden sind, konnten mit Hilfe der Kapazitäten im Schienengüterverkehr Versorgungsengpässe verhindert werden.

An vielen Stellen trägt der vorliegende Gesetzentwurf „zur Erhöhung der Sicherheit informationstechnischer Systeme" (IT-Sicherheitsgesetz 2.0) diesen und anderen Rahmenbedingungen Rechnung. So sind beispielsweise die **Informationspflichten** zu begrüßen. Demnach muss das Bundesamt für Sicherheit in der Informationstechnik (BSI) Betreiber Kritischer Infrastrukturen vor möglichen Risiken frühzeitig warnen. Zugleich beinhaltet der Gesetzentwurf aber auch Neuregelungen, die im Öffentlichen Personen- und Schienengüterverkehr zu erheblichen Mehrkosten, rechtlichen oder auch betrieblichen Risiken führen können. Das betrifft nicht nur den Eisenbahnverkehr, zu dem im Übrigen auch nicht-bundeseigene Bahnen gehören, sondern auch den Nahverkehr. Vor allem folgende Neuregelungen bedürfen einer Überarbeitung:

Der **§ 3** sieht gegenwärtig vor, dass die Entwicklung und Veröffentlichung von **sicherheitstechnischen Anforderungen an IT-Produkte** ausschließlich durch das BSI erfolgen soll. Da sich der Stand der Technik dynamisch durch etablierte Strukturen der nationalen, europäischen und internationalen Normung weiter entwickelt, besteht durch die angestrebte Regelung die Gefahr, dass die betroffenen Sektoren Kritischer Infrastrukturen von dieser Entwicklung abgekoppelt werden. In der Konsequenz können zum Beispiel die zur Erbringung der kritischen Dienstleistung erforderlichen Komponenten nicht mehr beschafft werden. So ist es sinnvoll, den Passus dahingehend zu ergänzen, dass der Stand der Technik wie bisher auf Basis anerkannter Normen und Standards ausgelegt wird, an deren Erarbeitung die betroffenen Sektoren Kritischer Infrastrukturen und die Wirtschafsverbände beteiligt sind.

Nachbesserungsbedarf wird darüber hinaus beim **§ 7b** gesehen. Demnach soll das BSI **Angriffssimulationen** auf gesetzlicher Basis durchführen dürfen. Der reinen automatisierten Detektion von Sicherheitslücken in IT-Systemen, die aus dem Internet heraus erreichbar sind, spricht nichts entgegen. Angriffssimulationen auf Betreiber Kritischer Infrastrukturen können aber zu Systemabstürzen führen, die die Erbringung der kritischen Dienstleistung gefährden bzw. unmöglich machen. Mögliche Haftungsansprüche aus diesem Vorgehen sind im vorliegenden Entwurf nicht geregelt. Es muss sichergestellt sein, dass es bei reinen Portscans bleibt und nicht weitere invasive Maßnahmen die Netz- und Informationssicherheit von betroffenen Betreibern gefährden.

Ferner enthält der Gesetzentwurf im **§ 8a (1a)** Anforderungen technischer Art, die praktisch nicht umsetzbar sind. Betroffene Unternehmen stünden vor nicht lösbaren Herausforderungen in rechtlicher und betrieblicher Hinsicht. So ist beispielsweise nicht nachvollziehbar, wie neue Systeme zur Angriffserkennung Störungen im Eisenbahn- oder Nahverkehr eigenständig beseitigen können sollen. Im Übrigen besteht für eine solche automatische Angriffserkennung und Gefahrenbeseitigung in den spezialgesetzlichen Regelungen zur Betriebsdurchführung keine rechtliche Grundlage. Anforderungen dieser Art sollten somit im weiteren Gesetzgebungsverfahren gestrichen werden.

Abschließend ist anzumerken, dass die mit der Gesetzesinitiative vermuteten Kostenbelastungen für die Wirtschaft gem. **E.2 (Erfüllungsaufwand**) nach den bisherigen Erfahrungen und vor dem Hintergrund der aufgewendeten Kosten in den betroffenen Unternehmen zu niedrig angesetzt sind.

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
19(4)727

UP KRITIS

Stellungnahme zum vorliegenden* Referentenentwurf des UP-KRITIS Wirtschaftsbeirates

Das Bundesinnenministerium hat am 09.12.2020 die Anhörung zum IT-Sicherheitsgesetz 2.0 von Zentral- und Gesamtverbänden sowie von Fachkreisen nach § 47 Absatz 3 der Gemeinsamen Geschäftsordnung der Bundesministerien eröffnet und bittet bis 10.12.2020, 14 Uhr um Beteiligung. Der UP KRITIS beteiligt sich mit seinem Mandat im Gesetzgebungsverfahren.

Die Wirtschaftsvertreter im UP KRITIS nehmen auf den folgenden Seiten Stellung zum Entwurf eines IT-Sicherheitsgesetzes 2.0 vom 09.12.2020. Eine fundierte Prüfung des im Rahmen der Verbändeanhörung veröffentlichten Dokuments ist in der Kürze der Zeit nicht leistbar. Daher basiert das Dokument auf einer Stellungnahme zu dem „Diskussionsentwurf“ vom 01.12.2020.

In diesem Dokument befinden sich keine Vorschläge für Neuformulierungen des Gesetzestextes. Aufgrund der sehr kurzen Frist zur Stellungnahme wird auf konkrete Textvorschläge zur Anpassung des Gesetzentwurfs verzichtet.

Inhalt:

Seite 2: Grundsätzliche Anmerkungen

Seite 3-4: „A. Kernaussagen“ zu dem Referentenentwurf in der uns vorliegenden Fassung
(beinhaltet ausschließlich die Kernaussagen)

Seite 5-10: „B. Stellungnahme“ des UP-KRITIS zu der jeweiligen Kernaussage
(beinhaltet Kernaussagen und Stellungnahmen)

Seite 11: Mitwirkende bei der Erstellung dieses Dokumentes (TAK Regulierung)

Dieses Dokument ist TLP Green eingestuft und kann somit an alle Unternehmen und Behörden, die Teilnehmer des UP KRITIS sind, zu deren Verwendung weitergegeben werden.

Grundsätzliche Anmerkungen

Die Wirtschaft im UP KRITIS begrüßt grundsätzlich die Weiterentwicklung des Ordnungsrahmens zum Schutz informationstechnischer Systeme von Kritischen Infrastrukturen. Die Art und Weise, wie das Bundesministerium des Innern, für Bau und Heimat das Gesetzgebungsverfahren durchführt, ist aus unserer Sicht inakzeptabel. Nach einer nunmehr zweijährigen Zeitspanne zur Erarbeitung eines Gesetzentwurfs werden die betroffenen Kreise im Rahmen der Verbändeanhörung mit einer Frist von knapp 25 Stunden zur Stellungnahme zu einem umfangreich und inhaltlich erweiterten Entwurf aufgefordert.

Angesichts der Relevanz der Informationssicherheit aus Sicht der Betreiber Kritischer Infrastrukturen und den tiefgreifenden Implikationen der angedachten gesetzlichen Neuerungen fordern wir die Bundesregierung auf, die betroffenen Kreise mit einer angemessenen Frist von mindestens zwei Wochen anzuhören. Es ist aus unserer Sicht zweifelhaft, wie das Bundesinnenministerium die in Zuge der laufenden Anhörung eingehenden Stellungnahmen annähernd würdigen und gegebenenfalls berücksichtigen kann.

Der UP KRITIS hat seine Stellungnahme vom 08.12.2020 nochmal überarbeitet und weist zusätzlich und nicht abschließend auf folgende Punkte zu dem Entwurf vom 09.12.2020 hin:

- Die Bundesregierung plant, diverse Übergangsfristen zur Umsetzung von Vorgaben, wie z.B. der Registrierung neuer Anlagen, zu streichen bei gleichzeitiger Verschärfung von Sanktionsmechanismen, die nicht mehr nur bei fahrlässigem oder vorsätzlichem Handeln verhängt werden können. Von diesem Zusammenspiel von gestrichenen Übergangsfristen und unmittelbaren Sanktionstatbeständen geht ein hohes Risiko von existenzgefährdenden Bußgeldern für betroffene Unternehmen aus, die bereits aufgrund von Bagatell-Verstößen verhängt werden können. Die Wirtschaftsvertreter im UP KRITIS fordern die Bundesregierung auf, den Gesetzentwurf im Sinne der Verhältnismäßigkeit von Bußgeldern zu Verstößen zu überarbeiten.

- Von einer Einführung von Pflichten zur Umsetzung spezifischer technischer Maßnahmen in einem abstrakten Gesetz sollte unbedingt Abstand genommen werden. Der Entwurf enthält Anforderungen technischer Art, die mit der Realität der Praxis wenig gemeinsam haben. Die Pflicht zur Umsetzung würde betroffene Kreise vor unklare und zum Teil nicht lösbare Herausforderungen stellen, weitere zusätzliche Gefährdungen mit sich bringen und in Konsequenz zu erheblicher Rechtsunsicherheit führen. Es ist nicht nachvollziehbar, wie z.B. Systeme zur Angriffserkennung eingetretene Störungen beseitigen können. Auch können informationstechnische Systeme nicht eigenständig Bedrohungen vermeiden. Sachfremde Anforderungen sollten aus dem Gesetzestext entfernt werden.

- Die unvermittelte Aufnahme des § 10 Absatz 6 erschließt sich uns nicht. Aufgrund der fehlenden Begründung können weder Sinn und Zweck noch die Implikationen für den Betrieb von informationstechnischen Systemen der Betreiber Kritischer Infrastrukturen abgeschätzt werden. Es ist davon auszugehen, dass die Befugnis des Bundesinnenministeriums zu einem weitreichenden Eingriff führen würde.

A. Kernaussagen:

1. **Von der Einholung der Garantieerklärung für kritische Komponenten, über deren Administration bis zu den potenziellen betrieblichen und wirtschaftlichen Folgeschäden durch die Einbeziehung von Behörden bis hin zur Untersagung eines Komponenteneinsatzes, müssten Betreiber die Auswirkungen tragen. Das Vorgehen greift durch die Zwangsvorgaben auch in das EU-Ausschreibungsrecht zu Lasten der betroffenen Unternehmen ein und führt ggf. zu Marktverzerrungen wegen Ungleichbehandlung. Die Kriterien zur Auswahl von einsetzbaren „kritischen Komponenten“ müssen zwingend festgelegt werden, um auf Betreiberseite Beschaffungsprozesse und die notwendige kurzfristige Reaktionsfähigkeit zur Aufrechterhaltung der Informationssicherheit auch im Gefahrenfall zu ermöglichen. Eine Untersagung des Einsatzes von bereits eingesetzten Komponenten zum Zeitpunkt des Inkrafttretens des Gesetzes muss ausgeschlossen werden (Bestandsschutz). Die angedachte Neuregelung birgt ansonsten die Gefahr die Informationssicherheit in Kritischen Infrastrukturen zu schwächen.**

2. **Es sind Prämissen für die Ausprägung von Systemen zur Angriffserkennung (Intrusion Detection) nach § 7b dargelegt. Allerdings ist die Heraustrennung von personenbezogenen Daten mit heutigen technischen Mitteln nicht angemessen leistbar. Das Vorhalten von für die Angriffserkennung und -nachverfolgung relevanten Daten über vier Jahre ist im Angesicht des erforderlichen Aufwands nicht verhältnismäßig (Archivierung und Speicherplatz). Wir schlagen eine Speicherzeit von bis zu 12 Monaten vor, analog der Ausführungen in § 5a Absatz 2.**

   Eine Übergangsfrist von mindestens zwei Jahren ist für die grundsätzliche Einführung von Systemen zur Angriffserkennung notwendig. Fristen (Umsetzung und Nachweis) sollten in allen Gesetzesanpassungen gleich gehandhabt werden (z.B. BSI-G = EnWG).

   Ein zielführender Einsatz von Systemen zur Angriffserkennung erfordert neben der Einführung von geeigneter Hard- und Software den Aufbau entsprechender Monitoring-, Detektions-, Analyse-, Alarmierungs- und Reaktionsprozesse im Unternehmen. Diese Aufgaben werden üblicherweise durch sogenannte Security Operation Center (SOC) wahrgenommen. Hierbei handelt es sich faktisch um den Aufbau von hochspezialisierten Teams, die 24/7 tätig sind. Der finanzielle und personelle Aufwand, der mit der Forderung nach Systemen zur Angriffserkennung einhergeht, ist beträchtlich und für die allermeisten KRITIS-Betreiber nicht leistbar.

   Der Anspruch des Gesetzgebers an den Einsatz solcher Systeme muss daher auf IT-technische Eigenschaften im Sinne von Mindestanforderungen begrenzt sein.

3. **Es ist begrüßenswert, dass sich das Strafmaß an einem europäischen Bußgeldrahmen orientiert. Das vorgeschlagene, abgestufte Sanktionsmaß erachten wir als grundsätzlich angemessen und sachgemäß. Der in den Bußgeldvorschriften neu eingeführte Verweis auf das Ordnungswidrigkeitengesetz, der zu einer Erhöhung um das 200-Fache des jetzigen Sanktionsmaßes von 100.000 € auf 20 Mio. € führen kann, muss gestrichen werden, da ein derart enormes Sanktionsmaß wiederum zu einer extremen Unverhältnismäßigkeit führt.**

   Da mit dem aktuellen Entwurf des IT-SiG 2.0 vom 09.12.2020 mehrere Übergangsfristen praktisch gestrichen wurden (z.B. die Registrierung neuer Anlagen) und gleichzeitig Bußgelder nicht mehr nur bei fahrlässigem oder vorsätzlichem Handeln verhängt werden können, besteht ein hohes Risiko von existenzgefährdenden Bußgeldern aufgrund von Bagatell-Verstößen.

4. **Der Erfüllungsaufwand für die Wirtschaft ist aus Sicht der Wirtschaft nicht nachvollziehbar beziffert: Pro Betreiber Kritischer Infrastruktur würde selbst auf Basis der optimistischen Schätzung der Bundesregierung von 21 Mio. € auf Seiten der Wirtschaft lediglich ein Aufwand von 10.800 € pro Unternehmen entstehen. Allein für die Speicherung von für die Angriffserkennung notwendigen Daten**

reicht weder für ein Jahr noch für die vorgeschlagenen vier Jahre aus. Der UP KRITIS weist auf die kürzlich durchgeführte Erhebung des Statistischen Bundesamts in den Sektoren der Kritischen Infrastrukturen hin, die der Abschätzung des Erfüllungsaufwands zugrunde gelegt werden sollte. Des Weiteren liegen weiterhin keine Entlastungsmaßnahmen für die Wirtschaft vor.

5. **„Unternehmen im besonderen öffentlichen Interesse“ sowie „erhebliche volkswirtschaftliche Schäden“ sind im Gesetzestext näher zu bestimmen, z.B. über einen direkten Verweis auf § 44 Absatz 1 GWB (sog. Hauptgutachten, siehe Begründung). Hierbei muss die Gleichbehandlung aller vom Gesetz betroffenen Unternehmen und die EU-Harmonisierung (keine Wettbewerbsnachteile) berücksichtigt werden. Wir weisen auf die Gefahr einer Doppelregulierung von Unternehmen der Sektoren der Kritischen Infrastrukturen hin, die über Tochtergesellschaften, die kritische Dienstleistungen erbringen, zusätzlich erfasst werden könnten. Doppelregulierungen müssen vermieden werden. Der UP KRITIS sollte zur Ausgestaltung der Rechtsverordnung nach § 10 Absatz 5 einbezogen werden.**

6. **Da als Basis weiterhin das Funktionieren des Gemeinwesen und die Gefährdung der öffentlichen Sicherheit herangezogen wird, muss der Gesetzgeber die von Unternehmen in der Regel geschaffenen Rückfallebenen und die Zeiträume von Ausfällen und Störungen zwingend mit betrachten (siehe auch EU NIS-Richtlinie), um die Kritikalität von IT-Störungen angemessen einschätzen zu können. Nur erhebliche Störungen von informationstechnischen Systemen mit Bezug zur Versorgung der Allgemeinheit sind meldepflichtig. Dieser Ansatz fehlt weiterhin im vorliegenden Entwurf.**

7. **Die Informationspflichten des BSI an die Betreiber Kritischer Infrastrukturen wurden in § 4b konkretisiert. Die Weitergabe von Erkenntnissen über Schwachstellen, Sicherheitslücken und weiteren Sicherheitsrisiken sollte allerdings unverzüglich, verpflichtend und unabhängig von weiteren Sicherheitsinteressen durch das BSI erfolgen.**

8. **Bei der Detektion von Sicherheitsrisiken für die Netz- und Informationssicherheit eines Betreibers Kritischer Infrastruktur durch das Bundesamt nach § 7b muss sichergestellt werden, dass es bei reinen Portscans bleibt und nicht weitere invasive Maßnahmen die Netz- und Informationssicherheit von betroffenen Betreibern gefährden.**
   Beim Einsatz von Honeypots muss wiederum sichergestellt werden, dass Informationen, die durch Maßnahmen nach § 7b Absatz 1 sowie Meldungen nach § 8b Absätze 4 und 4a erlangt wurden, nicht in die Architektur dieser Honeypots Einfluss finden (kein Aufbau von „Trainingsplattformen“ für Angreifer mit Bezug zu Kritischen Infrastrukturen). Der Ausschluss der Durchführung weitergehender, invasiver Maßnahmen durch das Bundesamt ist sachgemäß und vertrauensbildend.

9. **Die Entwicklung und Veröffentlichung von sicherheitstechnischen Anforderungen an IT-Produkte nach § 3 Absatz 1 Satz 2 Nummer 20 durch das Bundesamt darf nicht in einen nationalen Alleingang münden. Der Stand der Technik sollte wie bisher auf Basis anerkannter Normen und Standards ausgelegt werden, an deren Erarbeitung die betroffenen Sektoren Kritischer Infrastrukturen und deren Wirtschafsverbände beteiligt sind.**

10. **Es ist nicht nachvollziehbar, dass das Bundesinnenministerium – trotz des nunmehr zweijährigen Zeitraums zur Erarbeitung des vorliegenden Referentenentwurfs –die Durchführung der gesetzlich verankerten Pflicht zu Evaluierung des Gesetzes nicht plausibel dargelegt und erläutert hat. Die Bundesregierung sollte die bisher eingeführten Cyber- und IT-Sicherheitsmaßnahmen auf ihre Wirksamkeit überprüfen und darauf aufbauend transparent weiterentwickeln. Der UP KRITIS regt an, die Evaluierung unter Heranziehung eines wissenschaftlichen Sachverständigen und innerhalb der etablierten staatlich-wirtschaftlichen Zusammenarbeit vorzunehmen. Die formale Beteiligung der betroffenen Kreise darf nicht durch eine voreilige Einbringung des Gesetzentwurfs in das Bundeskabinett unterbleiben. Eine offizielle Verbändeanhörung bedarf einer ausreichenden Frist von mindestens zwei Wochen.**

B. Stellungnahmen:

1. **Kernaussage: Von der Einholung der Garantieerklärung für kritische Komponenten, über deren Administration bis zu den potenziellen betrieblichen und wirtschaftlichen Folgeschäden durch die Einbeziehung von Behörden bis hin zur Untersagung eines Komponenteneinsatzes, müssten Betreiber die Auswirkungen tragen. Das Vorgehen greift durch die Zwangsvorgaben auch in das EU-Ausschreibungsrecht zu Lasten der betroffenen Unternehmen ein und führt ggf. zu Marktverzerrungen wegen Bevorzugung/Benachteiligung. Die Kriterien zur Auswahl von einsetzbaren „kritischen Komponenten“ müssen zwingend festgelegt werden, um auf Betreiberseite Beschaffungsprozesse und die notwendige kurzfristige Reaktionsfähigkeit zur Aufrechterhaltung der Informationssicherheit auch im Gefahrenfall zu ermöglichen. Eine Untersagung des Einsatzes von bereits eingesetzten Komponenten zum Zeitpunkt des Inkrafttretens des Gesetzes muss ausgeschlossen werden (Bestandsschutz). Die angedachte Neuregelung birgt ansonsten die Gefahr, die Informationssicherheit in Kritischen Infrastrukturen zu schwächen.**

Bei der Untersagung des Einsatzes kritischer Komponenten nicht vertrauenswürdiger Hersteller sind gesetzlich weitere Maßnahmen vorzusehen, die für die Aufrechterhaltung der kritischen Geschäftsprozesse (trotz Untersagung) sorgen, realistische Übergangsfristen geben, die Pflicht zur Nennung von verfügbaren Austauschprodukten enthalten und eine langfristige Verhinderung der Monopolbildung für Produkte verhindern. Wir regen dringend an, diese Punkte bei der Gesetzgebung zu beachten.

Betreiber werden an Stelle des Gesetzgebers in die Pflicht genommen, beim Hersteller eine Garantieerklärung einzuholen, welche an das BMI gesendet werden soll. Die Verwaltung und Übermittlung von Garantieerklärungen stellen einen erheblichen Aufwand dar. Daraus ergibt sich kein Mehrwert für den effektiven Schutz Kritischer Infrastrukturen.

2. **Kernaussage: Es sind Prämissen für die Ausprägung von Systemen zur Angriffserkennung (Intrusion Prevention) nach § 8a Absatz 1a dargelegt. Allerdings ist das Vorhalten von für die Angriffserkennung und -nachverfolgung relevanten Daten über vier Jahr nach § 8a Absatz 1b im Angesicht des erforderlichen Aufwands nicht verhältnismäßig (Speicherplatz und Archivierung). Die Heraustrennung von personenbezogenen Daten mit heutigen technischen Mitteln ist nicht angemessen leistbar. Wir schlagen eine Speicherzeit im Normalfall von mindestens drei Monaten und bei Verdacht auf einen Angriff von bis zu 12 Monaten vor, analog der Ausführungen in § 5a Absatz 2.**

   Eine Übergangsfrist von mindestens zwei Jahren ist für die grundsätzliche Einführung von Systemen zur Angriffserkennung notwendig.

   Ein zielführender Einsatz von Systemen zur Angriffserkennung erfordert neben der Einführung von geeigneter Hard- und Software den Aufbau entsprechender Monitoring-, Detektions-, Analyse-, Alarmierungs- und Reaktionsprozesse im Unternehmen. Diese Aufgaben werden üblicherweise durch sog. Security Operation Center (SOC) wahrgenommen. Hierbei handelt es sich faktisch um den Aufbau von hochspezialisierten Teams, die 24/7 tätig sind. Der finanzielle und personelle Aufwand, der mit der Forderung nach Systemen zur Angriffserkennung einhergeht, ist beträchtlich und für die allermeisten KRITIS-Betreiber nicht leistbar.

   Der Anspruch des Gesetzgebers an den Einsatz solcher Systeme muss auf IT-technische Eigenschaften im Sinne von Mindestanforderungen begrenzt sein.

Für den verpflichtenden Einsatz von Systemen zur Angriffserkennung nach §8a Absatz 1a sind aus Sicht des UP KRITIS Prämissen für die Ausprägung dargelegt.

Der Aufbau eines umfassenden Systems zur Angriffserkennung (Aufbau und Betrieb von Security Operation Center - SOC) kann jedoch je nach Komplexität des Netzwerks und der Art der Vernetzung (oder Trennung) zu erheblichem Aufwand, insbesondere bzgl. Personalkapazitäten und den Betrieb erforderlicher Prozesse und Verfahren zur Reaktion auf Alarme führen.

Der UP KRITIS gibt zu bedenken, dass des Weiteren aufgrund der oben genannten Herausforderungen (Zeit, Personal, Know-How, Technik) anzunehmen ist, dass die Mehrheit der KRITIS-Betreiber hierzu einen Managed Security Services beauftragt. Da somit Zugang von wenigen Providern auf eine hohe Anzahl von Kritischen Infrastrukturen aufgebaut wird, müssen Angreifer auch nur noch wenige Provider zum Ziel haben, um größtmöglichen sektorübergreifenden Schaden zu verursachen. Dem muss unbedingt entgegengewirkt werden.

Kritisch zu sehen ist jedoch die Trennung personenbezogener Daten von nicht personenbezogenen Daten, da dies technisch nicht im angemessenen Verhältnis leistbar ist. Die Forderung einer Vorhaltung von Protokollierungsdaten über 4 Jahre würde den Aufbau eines technisch komplexen Archivierungssystems erfordern. Die zu erwartenden Mengen an anfallenden Protokollierungsdaten können in den Angriffserkennungssystemen selbst technisch nicht vorgehalten werden.

Der UP KRITIS schlägt eine Reduzierung der Speicherpflicht im Normalfall von mindestens drei Monaten und bei Verdacht auf einen Angriff von bis zu 12 Monaten vor. Dies orientiert sich an der Pflicht des Bundesamts zur Verarbeitung und Speicherung von behördeninternen Protokollierungsdaten nach § 5a Absatz 2, die als angemessen angesehen wird.

Im Angesicht der administrativen und finanziellen Aufwände für Archivierung und Speicherplatz erscheinen die Fristen aus Sicht des UP KRITIS daher nicht als angemessen. Eine Übergangsfrist von mindestens zwei Jahren ist auf Grund der zeitlichen Vorgaben und Restriktionen bei der Beschaffung und Einführung von Komponenten sowie der Bereitstellung von qualifiziertem Personal für den Betrieb von Systemen zur Angriffserkennung notwendig.

3. **Kernaussage: Es ist begrüßenswert, dass sich das Strafmaß an einem europäischen Bußgeldrahmen orientiert. Das vorgeschlagene, abgestufte Sanktionsmaß erachten wir als grundsätzlich angemessen und sachgemäß. Der in den Bußgeldvorschriften neu eingeführte Verweis auf das Ordnungswidrigkeitengesetz, der zu einer Erhöhung um das 200-Fache des jetzigen Sanktionsmaßes von 100.000 € auf 20 Mio. € führen kann, muss gestrichen werden, da ein derart enormes Sanktionsmaß wiederum zu einer extremen Unverhältnismäßigkeit führt.**

Es ist begrüßenswert, dass sich das Strafmaß an einem europäischen Bußgeldrahmen orientiert. Das vorgeschlagene, abgestufte Sanktionsmaß erachten wir als grundsätzlich angemessen und sachgemäß.

Der Verweis auf das Ordnungswidrigkeitengesetz für das Sanktionsmaß von 2 Mio. € bewirkt im Endeffekt ein Höchstmaß von 20 Mio. € bei Verstößen nach § 14 Absatz 2 Satz 1. Die Erhöhung des Höchstmaßes auf die Strafhöhe der Datenschutzgrundverordnung erscheint unverhältnismäßig, da es um Verstöße von Unternehmen gegen die Pflichten des IT-Sicherheitsgesetzes gilt und nicht um die Grundrechte von Bürgerinnen und Bürgern. Der UP KRITIS fordert die ersatzlose Streichung des Verweises auf das Gesetz über Ordnungswidrigkeiten.

Es ist ferner sicher zu stellen, dass es nicht zu einer Doppelregulierung /-bestrafung durch DSGVO und IT-SIG 2.0 kommen kann (sobald personenbezogene Daten betroffen sind).

4. **Der Erfüllungsaufwand für die Wirtschaft ist aus Sicht der Wirtschaft nicht nachvollziehbar beziffert. Er sollte gemäß der kürzlich durchgeführten Erhebung des Statistischen Bundesamts in den Sektoren der Kritischen Infrastrukturen dargelegt werden. Des Weiteren liegen weiterhin keine Entlastungsmaßnahmen für die Wirtschaft vor.**

Neben drohenden Bußgeldern, soll es nach Schätzung der Behörden durch das geplante Regelungsvorhaben der Bundesregierung für die Wirtschaft zu einmaligen Personalkosten von knapp 70.000 Euro sowie zu einer Veränderung der jährlichen Sach- und Personalkosten von 9 Millionen Euro kommen. Die Angaben sind nicht nachvollziehbar, da bereits heute ein deutlich höherer Aufwand betrieben werden muss, um die Verwaltungsanforderungen aus dem IT-SiG 1.0 zu erfüllen. Soweit durch das Regelungsvorhaben für die Wirtschaft zusätzlicher laufender Erfüllungsaufwand entsteht, soll dieser durch geeignete Entlastungsmaßnahmen kompensiert werden.

Der Erfüllungsaufwand für die Wirtschaft sollte gemäß der kürzlich durchgeführten Erhebung des Statistischen Bundesamts in den Sektoren der Kritischen Infrastrukturen beziffert werden. Des Weiteren liegen weiterhin keine Entlastungsmaßnahmen für die Wirtschaft vor.

Wir bitten um Vorlage von Erkenntnissen bezüglich der Erhebung des Statistischen Bundesamts in der Sache sowie um Benennung, welche Entlastungsmaßnahmen für die Wirtschaft vorgesehen sind und wann diese umgesetzt werden.

5. **Kernaussage: Unternehmen im besonderen öffentlichen Interesse“ sowie „erhebliche volkswirtschaftliche Schäden“ sind im Gesetzestext näher zu bestimmen, z.B. über einen direkten Verweis auf § 44 Absatz 1 GWB (sog. Hauptgutachten, siehe Begründung). Hierbei muss die Gleichbehandlung aller vom Gesetz betroffenen Unternehmen und die EU-Harmonisierung (keine Wettbewerbsnachteile) berücksichtigt werden. Wir weisen auf die Gefahr einer Doppelregulierung von Unternehmen der Sektoren der Kritischen Infrastrukturen hin, die über Tochtergesellschaften, die kritische Dienstleistungen erbringen, doppeltzusätzlich erfasst werden könnten. Doppelregulierungen müssen vermieden werden. Der UP KRITIS sollte zur Ausgestaltung der Rechtsverordnung nach § 10 Absatz 5 einbezogen werden.**

Eine Gleichbehandlung der Unternehmen ist nachvollziehbar sicherzustellen.

Um Wettbewerbsnachteile nationaler Unternehmen zu vermeiden, muss eine Harmonisierung mit der EU NIS-Richtlinie und der AEUV („AEUV fördert den Binnenmarkt, indem er alle Maßnahmen verbietet, die den freien Warenverkehr zwischen den Mitgliedstaaten behindern“) erfolgen.

Die Termini „Unternehmen im besonderen öffentlichen Interesse“ sowie „erhebliche volkswirtschaftliche Schäden“ sind näher zu bestimmen. Der Gesetzgeber sollte direkt im IT-Sicherheitsgesetz die Wesens-merkmale derartiger Infrastrukturen spezifizieren sowie inhaltlich von den Kritischen Intrastrukturen i.S.d. § 2 Abs. 10 BSIG abgrenzen und eine Risikoorientierung auf Basis von Sektorstudien, die mit den Branchenverbänden im jeweiligen Sektor abgestimmt sein müssen, als Grundlage heranziehen.

Betreiber, die durch die KritisV nicht erfasst sind (z.B. unter Schwellwerte), sollten nicht als „Unternehmen im besonderen öffentlichen Interesse“ erfasst und über diesen Weg dann reguliert werden.

6. **Kernaussage: Da als Basis weiterhin das Funktionieren des Gemeinwesen und die Gefährdung der öffentlichen Sicherheit herangezogen wird, muss der Gesetzgeber die von Unternehmen in der Regel geschaffenen Rückfallebenen und die Zeiträume von Ausfällen und Störungen zwingend mit betrachten (siehe auch EU NIS-Richtlinie), um die Kritikalität von IT-Störungen angemessen einschätzen zu können. Nur erhebliche Störungen von informationstechnischen Systemen mit Bezug**

zur Versorgung der Allgemeinheit sind meldepflichtig. Dieser Ansatz fehlt weiterhin im vorliegenden Entwurf.

7. Kernaussage: Die Informationspflichten des BSI an die Betreiber Kritischer Infrastrukturen wurden in § 4b konkretisiert. Die Weitergabe von Erkenntnissen über Schwachstellen, Sicherheitslücken und weiteren Sicherheitsrisiken sollte allerdings unverzüglich, verpflichtend und unabhängig von weiteren Sicherheitsinteressen durch das BSI erfolgen.

Wir begrüßen es, dass das BSI in die Lage versetzt werden soll, weiter ein bundesweites Lagebild zu erstellen und Betreiber über mögliche Risiken zu warnen. Dieses ist aber auch schon durch das IT-SIG 1.0 gegeben. Hier zusätzlich die Möglichkeit der Teilung von Erkenntnissen mit anderen Behörden einzuräumen (Erfüllungshilfe) entspricht nicht dem Sinne (Schutz Kritischer Infrastrukturen) dieses Gesetzes und ist zu überdenken.

Der UP KRITIS begrüßt grundsätzlich auch die in §4b konkretisierten Informationspflichten des BSI an die Betreiber. Sollte das BSI durch Meldungen von Betreibern, anderen nationalen CIRTs (EU NIS-Richtlinie) oder anderen Behörden (z.B. Verfassungsschutz) Erkenntnisse über Schwachstellen oder Bedrohungen gewinnen, muss es diese Erkenntnisse jedoch verpflichtend und unverzüglich den betroffenen Unternehmen zukommen lassen. Nur zügig geschlossene Schwachstellen stärken die Cyberresilienz Deutschlands. Dieser Aspekt ist in die Konkretisierung aufzunehmen und entsprechend auszugestalten.

8. Kernaussage: Vor der Detektion von Sicherheitsrisiken für die Netz- und Informationssicherheit eines Betreibers Kritischer Infrastruktur durch das Bundesamt nach § 7b sollte eine Abstimmung mit dem betroffenen Betreiber unverzüglich und ohne Ausnahmen erfolgen.
Angriffssimulationen vom BSI auf Betreiber Kritischer Infrastrukturen können zu Systemabstürzen führen. Sie müssen auf Schwachstellendetektion eingeschränkt werden. Zudem muss die Haftung, für die durch Schwachstellenanalysen ggf. hervorgerufenen Schäden, geklärt werden. Beim Einsatz von Honeypots muss ausgeschlossen werden, dass Kennungen von informationstechnischen Systemen von Betreibern Kritischer Infrastruktur durch das Bundesamt genutzt werden. Der Ausschluss der Durchführung weitergehender, invasiver Maßnahmen durch das Bundesamt ist sachgemäß und vertrauensbildend.

Zukünftig soll das BSI Angriffssimulationen auf gesetzlicher Basis durchführen dürfen. Der reinen automatisierten Detektion von Sicherheitslücken in IT-Systemen, die aus dem Internet heraus erreichbar sind, spricht nichts entgegen. Schon heute werden tagtäglich sogenannte „Portscans“ millionenfach aus allen möglichen Quellen heraus vorgenommen.

Der Gesetzestext schränkt den Umfang der Angriffssimulation auf die Durchführung von „Portscans“ ein, d.h. weiterführende, invasive Maßnahmen wie „Penetrationsanalysen“ durch das Bundesamt sind gesetzlich ausgeschlossen.

Bei dem Einsatz von Systemen und Verfahren des BSI, welche einem Angreifer einen erfolgreichen Angriff vortäuschen (Honeypot, Artikel 1 § 7b (4) BSI-G) muss im Gesetz geregelt sein, dass der Einsatz von branchenspezifischen Lösungen (z.B. Produktionsanlagen, Industrielle Kontrollsysteme) mit den Betreibern abgestimmt sein muss, um hier keine „Lernplattform“ für Angreifer zu schaffen.

9. Kernaussage: Die Entwicklung und Veröffentlichung von sicherheitstechnischen Anforderungen an IT-Produkte nach § 3 Absatz 1 Satz 2 Nummer 20 durch das Bundesamt darf nicht in einen nationalen Alleingang münden. Der Stand der Technik sollte wie bisher auf Basis anerkannter Normen und Standards ausgelegt werden, an deren Erarbeitung die betroffenen Sektoren Kritischer Infrastrukturen und deren Wirtschafsverbände beteiligt sind.

Betreiber Kritischer Infrastrukturen sind nach § 8a BSIG verpflichtet zur Umsetzung von technischen und organisatorischen Maßnahmen nach dem Stand der Technik. Die Betreiber Kritischer Infrastrukturen sind daher als unmittelbar Betroffene bei der Entwicklung eines Stands der Technik bei sicherheitstechnischen Anforderungen an IT-Produkte einzubeziehen, analog zu Beteiligungsmöglichkeiten in der nationalen, europäischen und internationalen Normung.

Der Stand der Technik entwickelt sich dynamisch weiter und wird durch etablierte Strukturen der nationalen, europäischen und internationalen Normung entwickelt. Betroffene und interessierte Kreise sind hieran beteiligt. Es darf keine Abkehr von diesen etablierten Verfahren insbesondere von branchenspezifischen Sicherheitsstandards (B3S) geben, die in einen nationalen Alleingang in der Sache münden würde. Zertifizierungen, die nach dem Stand der Technik anderer Organisationen bzw. Branchenverbänden für Informationssicherheit erfolgen, sind ebenfalls anzuerkennen. Ein Verbot von bereits im Einsatz befindlichen Komponenten muss vermieden werden.

Der UP KRITIS schlägt vor, den Passus dahingehend zu ergänzen, dass ein Stand der Technik unter Berücksichtigung von bestehenden, anerkannten Normen und Standards erfolgen muss unter Beteiligung der betroffenen Sektoren Kritischer Infrastrukturen und deren Wirtschaftsverbände.

10. Kernaussage: Es ist nicht nachvollziehbar, dass das Bundesinnenministerium – trotz des nunmehr zweijährigen Zeitraums zur Erarbeitung des vorliegenden Referentenentwurfs –die Durchführung der gesetzlich verankerten Pflicht zu Evaluierung des Gesetzes nicht plausibel dargelegt und erläutert hat. Die Bundesregierung sollte die bisher eingeführten Cyber- und IT-Sicherheitsmaßnahmen auf ihre Wirksamkeit überprüfen und darauf aufbauend transparent weiterentwickeln. Der UP KRITIS regt an, die Evaluierung unter Heranziehung eines wissenschaftlichen Sachverständigen und innerhalb der etablierten staatlich-wirtschaftlichen Zusammenarbeit vorzunehmen. Die formale Beteiligung der betroffenen Kreise darf nicht durch eine voreilige Einbringung des Gesetzentwurfs in das Bundeskabinett unterbleiben. Eine offizielle Verbändeanhörung bedarf einer ausreichenden Frist von mindestens zwei Wochen.

Generell erkennen die am UP KRITIS teilnehmenden Unternehmen nur ansatzweise, dass Erfahrungen aus der Umsetzung des IT-SiG 1.0 sowie Erkenntnisse und Rückmeldungen von KRITIS-Betreibern in die aktuelle Fassung des Referentenentwurfs eingeflossen sind. Es ist nicht nachvollziehbar, dass das Bundesinnenministerium – trotz des nunmehr zweijährigen Zeitraums zur Erarbeitung des vorliegenden Referentenentwurfs –der gesetzlich verankerten Pflicht zu Evaluierung des Gesetzes nicht nachgekommen zu sein scheint.

Der UP KRITIS empfiehlt, den vorliegenden Referentenentwurf so zu überarbeiten, dass Änderungen am IT-SiG nachvollziehbar aus den gewonnenen Erkenntnissen („Lessons Learned“) resultieren, die im Zuge der Evaluation gewonnen werden müssten.

Die formale Beteiligung der betroffenen Kreise darf nicht durch eine voreilige Einbringung des Gesetzentwurfs in das Bundeskabinett unterbleiben. Eine offizielle Verbändeanhörung bedarf einer ausreichenden Frist von mindestens zwei Wochen.

Der UP KRITIS sieht Wettbewerbsnachteile und Einschränkungen der unternehmerischen Freiheit der Betreiber und empfiehlt, dies aktiv abzuwenden. Wirtschafts- und geopolitische Interessen dürfen nicht auf dem Rücken der nationalen Betreiber ausgetragen werden.

Die zugrundeliegenden Abwägungen bedürfen generell einer nachvollziehbaren Erläuterung.

Weitreichende Datenschutz- und Geschäftsgeheimnisschutz-Aspekte im IT-SiG 2.0 verkomplizieren die zugrundeliegende Gesetzgebung (DSGVO, GeschGehG) und sollten daher in gesonderten Artikeln des IT-SiG 2.0 zusammengeführt und in den jeweils zugrundeliegenden Gesetzen vorgenommen werden (Änderung des Umsetzungsgesetzes der DSGVO sowie des GeschGehG, anstatt Änderungen an TKG, TMG, BSIG).

Mitglieder des Themenarbeitskreises (TAK) Regulierung und Ersteller_innen dieses Dokumentes

Vertreter_innen aus 8 Wirtschaftssektoren:
Finanz und Versicherungswesen, Transport und Verkehr, IT und TK, Wasser, Gesundheit, Energie (Strom/Gas/Fernwärme), Ernährung, Medien und Kultur

TAK Mitglied		Unternehmen
Albrecht	Frank	REWE Systems GmbH
Bleschke	Sebastian	Initiative Erdgasspeicher e.V.
Bendjebbour	Yassin	Bundesverband der Energie- und Wasserwirtschaft e.V. (Energie)
Berndt	Andreas	50 Hertz GmbH
Bott	Daniel	AXA
Dambach	Stephan	Stadtwerke Speyer GmbH
Ebner	Michael	EnBW Energie Baden-Württemberg AG
Freudensprung	Rolf	Deutsche Lufthansa AG
Heiko	Hußmann	Landeshauptstadt Hannover
Huber	Hermann	Hubert Burda Media Holding KG
Jensen	Ingo	Bayernwerk Netz GmbH
Jochem	Rainer	Saarländischer Rundfunk
Junker	Wolfgang	Südzucker
Jünger	Andreas	Berliner Verkehrsbetriebe AöR
Kaminski	Peter	Santander Consumer Bank AG
Kastl	Andreas	Verband der Auslandsbanken in Deutschland e.V.
Kibittel	Petra	MEDIA BROADCAST GmbH
Knosowski	Yvonne	Kreiskliniken Gummersbach-Waldbröl GmbH
Kopper	Christoph	Sparkasse Lörrach-Rheinfelden
Krauhausen	Thomas	innogy SE
Kršić	Boban	DENIC eG
Mizera	Sascha	Südzucker
Münster	Enno	Deutsche Lufthansa AG
Marcus	Popp	EDEKA
Nash	André	Bundesverband deutscher Banken e.V.
Prechtel	Andreas	Verband der Auslandsbanken in Deutschland e.V.
Sabet	Stefanie	Bundesvereinigung der Deutschen Ernährungsindustrie e.V.
Sachgau	Christian	Deutsche Telekom AG
Saxena	Sunita-Ute	T-Systems International GmbH
Schmitz	Michaela	Bundesverband der Energie- und Wasserwirtschaft e.V. (Wasser)
Schulte	Gisbert	Bochum-Gelsenkirchener Straßenbahnen
Schützler	Michael	frischli Milchwerke GmbH
Sieck	Gabriele	Gesamtverband der deutschen Versicherungswirtschaft e.V.
Simon	Frank	Zürich Gruppe Deutschland
Stoffel	Matthias	SIZ GmbH
Stracke	Ralf	EWE AG
Van den Berg	Hans-Rainer	van den Berg Service AG
Wagner	Kirsten	Deutscher Verein des Gas- und Wasserfaches e.V.
Weise	Sven	Currenta
Wirtz	Frank	ERGO Group AG

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
19(4)728

BUNDESVERBAND PAKET & EXPRESS LOGISTIK BIEK

Stellungnahme

BSI-Gesetz – Sicherheit erhöhen ohne Bürokratie auszubauen

Der Deutsche Bundestag ist mit der ersten Lesung des IT-Sicherheitsgesetzes 2.0 (IT-SiG 2.0) in das Gesetzgebungsverfahren eingetreten. Wir möchten mit dieser Stellungnahme auf Aspekte aufmerksam machen, die aus unserer Sicht im parlamentarischen Verfahren nachgebessert werden sollten, um das Gesetz rechtssicher und effektiver zu gestalten.

Der Bundesverband Paket und Expresslogistik vertritt bundesweit tätige Paketdienstleister. Im Zusammenhang mit der aktuellen Sicherheitsdiskussion halten wir es für möglich, dass eine Diskussion auftritt, den Anwendungsbereich über den in der Begründung genannten Bereich hinaus auszudehnen, auch wenn hierfür kein Anlass besteht.

Eine grundsätzliche Anmerkung betrifft die Evaluierung bestehender Regelungen. Der Gesetzgeber hat eine Evaluierung des IT-Sicherheitsgesetzes im Gesetz selbst vorgesehen. Dennoch ist diese Evaluierung durch das Bundesministerium des Inneren, für Bau und Heimat (BMI) und das Bundesamt für Sicherheit in der Informationstechnik (BSI) unterblieben, zumindest ist uns keine Berichterstattung dazu bekannt.

Wir weisen in diesem Zusammenhang auf die Empfehlungen des UP-KRITIS hin. Es ist grundsätzlich fragwürdig, eine Verpflichtung zur Evaluierung im Gesetz vorzunehmen, sie dann aber nicht erkennbar vorzunehmen, Empfehlungen zur Weiterentwicklung zu ignorieren, aber dennoch eine Neuregelung vorzunehmen.

Konkrete Ansatzpunkte sehen wir bei den folgenden Aspekten:

1. Risikobezug

Weder das BMI noch das BSI haben eine Gefährdungsanalyse des Mobilitäts- und Logistiksektors vorgelegt, mit dem die Risiken aufzeigt, bewertet und darauf ausgerichtete gezielte Maßnahmen vorgeschlagen werden. Ziel muss es sein, die begrenzten Mittel zur Abwehr von Gefahren so gezielt einzusetzen, dass ein sehr hoher Sicherheitsstandard erlangt werden kann. Dafür müssen die größten Gefahren ermittelt und anschließend regulatorische Maßnahmen auf Basis eines risikobasierten Ansatzes entwickelt werden.

2. Verwendung unbestimmter Rechtsbegriffe

Im Gesetzentwurf werden unbestimmte Rechtsbegriffe verwendet, die im Ergebnis zu einseitig hohen Kostenrisiken der Wirtschaft führen, ohne den gewünschten Sicherheitseffekt erzielen zu können. So sind die im aktuellen Gesetzentwurf neu eingefügten Begriffe „Unternehmen im besonderen öffentlichen Interesse" sowie „erhebliche volkswirtschaftliche Schäden" näher zu bestimmen. Der Versuch einer näheren Bestimmung von „Wertschöpfung" bezieht sich z. B. nur auf deutsche

Unternehmen, nicht aber, was dem Zweck des Gesetzes eher entspräche, auf die Wertschöpfung auf dem Gebiet der Bundesrepublik Deutschland. Es gibt einen Klärungsbedarf bei der Definition, die in diesem Fall ein Maß (Wertschöpfung) ohne Bezug zum originären Schutzzweck der Vorschriften (Versorgungssicherheit der Bevölkerung in Deutschland) einführt. Auch die Vorgabe, IT-Systeme nach dem „Stand der Technik" vorzuhalten, ist genauer festzulegen. Hierbei muss die Gleichbehandlung aller vom Gesetz betroffenen Unternehmen und die EU-Harmonisierung (keine Wettbewerbsnachteile) berücksichtigt werden.

3. Unverhältnismäßige Sanktionsdrohungen

Unternehmen, die in den Anwendungsbereich des Gesetzes fallen, werden mit der Androhung hoher Strafzahlungen konfrontiert. Welche Unternehmen betroffen sein könnten, ist jedoch unklar, sodass der Großteil der deutschen Wirtschaft vorauseilend tätig werden müsste, um die hohen Bußgelddrohungen zu vermeiden. Der in den Bußgeldvorschiften neu eingeführte Verweis auf das Ordnungswidrigkeitengesetz kann das aktuelle Sanktionsmaß von 100.000 Euro auf 20 Millionen Euro, also um das 200-Fache erhöhen. Das halten wir für unverhältnismäßig und korrekturbedürftig.

Die Paketdienste investieren laufend in Digitalisierung und in sichere IT-Systeme, die schon im eigenen Interesse auch geprüft werden. Die mit dem Entwurf vorgeschlagenen Vorschriften und der pauschale Ansatz des Gesetzentwurfes verursachen jedoch einen erheblichen zusätzlichen Verwaltungsaufwand zudem werden personelle und finanzielle Kapazitäten gebunden, die dringend für die weitere Optimierung der Systeme gebraucht werden.

Vier Beispiele hierzu:

- Stand der Technik: Die pauschale Vorgabe, den „Stand der Technik" einzusetzen verpflichtet, immer das neueste Betriebssystem zu erwerben, auch wenn für die Vorgängerversion Sicherheitsupdates verfügbar und ihre Anwendung vereinbart ist. Das ist unwirtschaftlich und bindet unnötige Ressourcen.

- Anwenderhaftung: Durch die Ausrichtung auf Anwender und nicht auf Systemanbieter verlagert das Gesetz das Risiko auf die Nutzer von Soft- und Hardware, statt auf die Anbieter. Bei Fehlern des Soft- oder Hardwareanbieters können diese nicht in Haftung genommen werden. Sinnvoller ist der Ansatz „Security by Design", bei dem sichere Systembausteine zertifiziert und geprüft und deren Anbieter in Haftung genommen werden können. Betreiber kritischer Infrastrukturen, die beispielsweise Opfer des Mitte Dezember 2020 bekannt gewordenen Hackerangriffs auf den amerikanischen IT-Dienstleister SolarWinds wurden, müssen für den entstandenen Schaden selbst aufkommen. Solange im IT-Sicherheitsgesetz kein Verursacherprinzip hinterlegt ist, fehlt der Druck auf Hersteller Sicherheitslücken zu schließen.

- Meldeverfahren: Sobald eine Sicherheitslücke bekannt wird, sollten Betreiber kritischer Infrastrukturen schnellstmöglich darüber informiert werden, um eventuell nötige Vorkehrungen treffen zu können. Allerdings teilt das BSI scheinbar nur verzögert und nur ausgewählte Informationen. Damit bleibt die Schutzfunktion das BSI für die betroffene Wirtschaft lückenhaft.

- Bürokratieaufbau: Im Gesetzesentwurf wird der Anwendungsbereich des Gesetzes auf 2.000 Unternehmen geschätzt. Dem stehen auf der Verwaltungsseite alleine im BSI bis zu 200 zusätzliche Stellen gegenüber, was einem „Betreuungsverhältnis" alleine für das Melde- und Berichtswesen von 1 Mitarbeiter*in zu 10 Unternehmen entspricht.

Abschließend verweisen wir auf die zuvor genannten, bereits frühzeitig gegenüber dem BMI kommunizierten Vorschläge des UP KRITIS-Wirtschaftsrats zur Verbesserung des Gesetzentwurfs, denen wir uns anschließen.

Berlin, 10. Februar 2021

Deutscher Bundestag

Ausschuss für Inneres und Heimat

Ausschussdrucksache
19(4)740

Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme

Die Versicherungswirtschaft begrüßt das Vorhaben der Bundesregierung, die Cyberresilienz Deutschlands zu stärken. Die zunehmende Digitalisierung von Staat, Wirtschaft und Gesellschaft baut auf Cyber- und IT-Sicherheit auf und erfordert eine Kooperation aller Akteure.

Nachfolgende Punkte zur Verbesserung des von der Bundesregierung vorgelegten Gesetzentwurfs schlagen wir vor:

Festlegen des Standes der Technik (§ 3 Absatz 1 Nummer 20)

Der Gesetzentwurf sieht vor, dass das BSI die Entwicklung des Standes der Technik bzgl. Sicherheit von IT-Produkten übernehmen soll.

Dabei ist jedoch zu bedenken:

- Der Stand der Technik entsteht durch Agieren der Entwickler, Hersteller und Nutzer und ist einer sich ständig ändernden Dynamik ausgesetzt, die der Gesetzgeber bzw. eine Behörde nicht beeinflussen sollte.
- Es gibt bereits ausreichend kompetente Akteure am Markt, die sich laufend einer Beschreibung widmen und zum Stand der Technik veröffentlichen.
- Ein festgelegter Stand der Technik könnte Hersteller und deren Produkte ausschließen, die vor dem Festlegen genutzt werden konnten. Dadurch würde nur noch die Nutzung von Produkten gewisser Hersteller ermöglicht werden.

Daher sollte der Stand der Technik nicht durch das BSI festgelegt werden, sondern vielmehr – wie in der Praxis bewährt - dessen Beschreibung durch kompetente Institutionen erfolgen und so ohne bürokratische Aufwände den aktuellen Gegebenheiten angepasst werden.

Detektion von Sicherheitsrisiken für die Netz- und IT-Sicherheit und von Angriffsmethoden (§ 7b)

Das BSI soll durch § 7b BSIG-E in die Lage versetzt werden, zur „Detektion von Sicherheitslücken und anderen Sicherheitsrisiken an den Schnittstellen öffentlich erreichbarer informationstechnischer Systeme zu öffentlichen Telekommunikationsnetzen Maßnahmen (Portscans) durchzuführen, …“.

Dabei ist jedoch zu bedenken:

- Die Sicherheit und Verfügbarkeit der Systeme könnte durch den Scan gefährdet werden, da dem BSI im Vorfeld nicht klar sein kann, wie weit es durch die Detektion in die Systeme eindringt. Zudem ist die Haftung für Schäden nicht geregelt, die durch die Detektion verursacht werden.
- Neben den Haftungsfragen muss auch geklärt werden, wie die betroffenen Betreiber im Vorfeld über Umfang, Form und Zeitraum der Detektion informiert werden, wie das BSI die Detektion nachvollziehbar dokumentiert und garantiert, dass keine Hintertür verbleibt.

Die Maßnahmen müssen sich auf das absolut Notwendige zur Detektion der Sicherheitslücken beschränken, dürfen nicht über einen Portscan hinausgehen, und eine Kompromittierung der Systeme muss ausgeschlossen sein.

Untersagung des Einsatzes kritischer Komponenten (§ 9b)

Nach § 9b BSIG-E ist vorgesehen, Betreiber Kritischer Infrastrukturen zu verpflichten, dem BMI den Einsatz kritischer Komponenten anzuzeigen und nur kritische Komponenten von Herstellern einzusetzen, die eine Garantieerklärung der Vertrauenswürdigkeit über die gesamte Lieferkette hinweg abgeben (Abs. 2). Während der einmonatigen Prüfung der Komponenten soll deren Einsatz nicht gestattet sein (Abs.3). Zudem ist vorgesehen, dass da BMI den Einsatz bereits eingebaute kritischer Komponenten untersagen kann (Abs. 3).

Dabei ist jedoch zu bedenken:

- Gerade bei global hergestellten, komplexen Produkten ist die Lieferkette nicht immer zurückverfolgbar, eine Garantieerklärung über die gesamte Lieferkette daher nicht möglich.
- Die Möglichkeit einer nachträglichen Untersagung durch den Entzug der Vertrauenswürdigkeit und damit verbundene Rückbauverpflichtungen von bereits eingesetzten IT-Produkten sorgt für Rechtsunsicherheit und könnte im Extremfall eine Bedrohung der unternehmerischen Existenz darstellen.
- Die Betreiber müssten das Kostenrisiko eines angeordneten Rückbaus allein tragen und hierfür erhebliche Rückstellungen bilden. Daher müssten mindestens klare Verantwortlichkeiten, Ausstiegsszenarien und Übergangsfristen Rechtssicherheit garantieren, da es sonst zu erheblichen negativen Auswirkungen sowie rechtlichen Unsicherheiten kommen könnte.
- Ebenfalls berücksichtigt der Gesetzentwurf nicht, dass die Sicherheit technischer Produkte bereits durch das Ergreifen zusätzlicher organisatorischer und technischer Maßnahmen nachjustiert werden kann.
- Zudem sind die Folgen für die Versicherer und deren Geschäftsprozesse im Falle der Weigerung der Hersteller, eine Garantieerklärung abzugeben, unabsehbar. Darüber hinaus besteht die Gefahr einer Marktverzerrung, falls nur eine gewisse Anzahl an Herstellern eine solche Garantieerklärung für die gesamte Lieferkette abgeben. Dies könnte dazu führen, dass Versicherer sich in eine Abhängigkeit von diesen Herstellern begeben müssten.

Angesichts der aufgezeigten erheblichen Unsicherheiten, Konzentrationsrisiken und Mehraufwendungen sollte § 9b des BSIG-E in seiner jetzigen Form erheblich angepasst werden.

Der GDV hatte bereits zum Referentenentwurf eine Stellungnahme abgegeben, die Sie unter folgendem Link finden können:
[Stellungnahme]

Gesamtverband der Deutschen Versicherungswirtschaft e. V.

Wilhelmstraße 43 / 43 G, D-10117 Berlin
Postfach 08 02 64, D-10002 Berlin
Tel.: +49 30 2020-5000
Fax: +49 30 2020-6000

51, rue Montoyer
B - 1000 Brüssel
Tel.: +32 2 28247-30
Fax: +49 30 2020-6140
ID-Nummer 6437280268-55

Ansprechpartner:
Patrik Maeyer
Gabriele Sieck

E-Mail: **g.sieck@gdv.de**

www.gdv.de

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
19(4)743

Stellungnahme der Bundesärztekammer

zum Entwurf eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (BT-Drucksache 19/26106)

Berlin, 24.02.2021

Korrespondenzadresse:

Bundesärztekammer
Herbert-Lewin-Platz 1
10623 Berlin

Inhaltsverzeichnis

1. Grundlegende Bewertung des Gesetzesentwurfs 3
2. Stellungnahme im Einzelnen 3
Geltungsbereich der Mindeststandards für die Sicherheit der Informationstechnik des Bundes (§ 8 Abs. 1 S. 1 Nr. 2 BSI-Gesetz) 3

1. Grundlegende Bewertung des Gesetzesentwurfs

Das Gesetz will die Sicherheit der Informationstechnik des Bundes stärken und dabei neuen Bedrohungen und der zunehmenden Bedeutung der Informations- und Kommunikationstechnologie Rechnung tragen. Damit soll ein wichtiger Eckpunkt aus dem am 12. März 2018 abgeschlossenen Koalitionsvertrag umgesetzt werden. Die Bundesärztekammer unterstützt diese Zielsetzung im Grundsatz, gerade auch im Hinblick auf die zunehmende Digitalisierung und die aktuellen Herausforderungen durch die Corona-Pandemie.

2. Stellungnahme im Einzelnen

Geltungsbereich der Mindeststandards für die Sicherheit der Informationstechnik des Bundes (§ 8 Abs. 1 S. 1 Nr. 2 BSI-Gesetz)

A) Beabsichtigte Neuregelung

Nach § 8 Abs. 1 S. 1 BSI-Gesetz geltender Fassung erarbeitet das Bundesamt für Sicherheit in der Informationstechnik Mindeststandards für die Sicherheit der Informationstechnik des Bundes. Das BMI kann im Benehmen mit dem IT-Rat diese Mindeststandards ganz oder teilweise als allgemeine Verwaltungsvorschriften „für alle Stellen des Bundes“ erlassen.

Geplant ist nunmehr, sowohl den Adressatenkreis zu erweitern als auch die Verbindlichkeit der Mindeststandards zu erhöhen. Abweichungen von den Mindeststandards sollen nur noch in sachlich gerechtfertigten Fällen zulässig sein, wobei dies zu dokumentieren und zu begründen ist. Vom Anwendungsbereich sollen nach § 8 Abs. 1 S. 1 Nr. 2 BSI-Gesetz auch

> *„Körperschaften […] des öffentlichen Rechts sowie ihrer Vereinigungen ungeachtet ihrer Rechtsform auf Bundesebene, soweit von der jeweils zuständigen obersten Bundesbehörde angeordnet“*

erfasst werden.

B) Stellungnahme der Bundesärztekammer

Die Änderung wird in der vorliegenden Entwurfsfassung abgelehnt, weil der Anwendungsbereich unklar ist.

Die Bundesärztekammer ist als Arbeitsgemeinschaft der Landesärztekammern die Spitzenorganisation der ärztlichen Selbstverwaltung auf Bundesebene. Während die Landesärztekammern als Körperschaften des öffentlichen Rechts organisiert sind, haben sie sich auf Bundesebene in der Rechtsform eines nicht eingetragenen Vereins zusammengeschlossen. Die Bundesärztekammer vertritt die berufspolitischen Interessen der Ärztinnen und Ärzte in der Bundesrepublik Deutschland. Als Arbeitsgemeinschaft der 17 deutschen Ärztekammern wirkt sie aktiv am gesundheitspolitischen Meinungsbildungsprozess der Gesellschaft mit und entwickelt Perspektiven für eine bürgernahe und verantwortungsbewusste Gesundheits- und Sozialpolitik.

Die Bundesärztekammer unterliegt, weil sie keine staatlichen Aufgaben wahrnimmt, keiner Aufsicht durch oberste Bundesbehörden. Auch nimmt sie, wie aus Vorstehendem ersichtlich, keine Aufgaben wahr, die es erforderlich machen würden, die für kritische Infrastrukturen geltenden Mindestanforderungen zu erfüllen. Die Bundesärztekammer ist nicht Teil der (mittelbaren) Bundesverwaltung.

C) Änderungsvorschlag der Bundesärztekammer

§ 8 wird wie folgt geändert:

a) Absatz 1 wird durch die folgenden Absätze 1 und 1a neu ersetzt:

> *„(1) Das Bundesamt legt im Einvernehmen mit den Ressorts Mindeststandards für die Sicherheit der Informationstechnik des Bundes fest, die von*
>
> *1. Stellen des Bundes,*
>
> *2. Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts* ***sowie ihrer hoheitliche Aufgaben wahrnehmenden*** *Vereinigungen ungeachtet ihrer Rechtsform auf Bundesebene, soweit von der jeweils zuständigen obersten Bundesbehörde angeordnet, sowie*
>
> *3. öffentlichen Unternehmen, die mehrheitlich im Eigentum des Bundes stehen und die IT-Dienstleistungen für die Bundesverwaltung erbringen,*
>
> *umzusetzen sind. […]“*

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
19(4)744

DEUTSCHE KRANKENHAUS GESELLSCHAFT

Bundesverband der Krankenhausträger in der Bundesrepublik Deutschland

Stellungnahme

der Deutschen Krankenhausgesellschaft

zum

Entwurf der Bundesregierung

eines

Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-SiG 2.0)

Bundestag-Drucksache 19/26106

vom 24. Februar 2021

Inhaltsverzeichnis

Allgemeiner Teil 3

Besonderer Teil 5

Artikel 1 Änderung des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) 5

Zu Artikel 1 Nummer 12 Buchstabe b (§ 8a Absatz 1a BSIG – neu)
Verpflichtung zur Vorhaltung von Systemen zur Angriffserkennung sowie Protokollierung entsprechender Information 5

Zu Artikel 1 Nummer 22 (§ 14 BSIG – neu)
Bußgeldvorschriften 7

Weiterer gesetzlicher Handlungsbedarf 8

Allgemeiner Teil

Das Bundesministerium des Innern, für Bau und Heimat (BMI) hat am 03.12.2020 den noch nicht innerhalb der Ressorts abgestimmten Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-SiG 2.0) auf seiner Webseite veröffentlicht. Zunächst hat das BMI nicht die übliche Möglichkeit zur Anhörung der Verbände eingeräumt und stattdessen lediglich um eine allgemeine Rückmeldung zum Gesetzentwurf bis zum 09.12.2020 (zunächst 06.12.2020) gebeten. Kurzfristig wurde der umfangreiche Referentenentwurf Verbänden mit einer eintägigen Stellungnahmefrist übersandt. Der Regierungsentwurf wurde dann am 16.12.2020 erneut mit der Aufforderung zur Stellungnahme versandt. Eine inhaltliche Auseinandersetzung mit den Stellungnahmen zum Referentenentwurf war dem BMI in der Zwischenzeit nicht möglich.

Es ist richtig, angesichts der wachsenden Digitalisierung auch im Gesundheitswesen die gesetzlichen Rahmenbedingungen zum Schutz vor Cyberangriffen weiterzuentwickeln und dabei den notwendigen Diskurs mit allen hieran Beteiligten zu suchen, auch um Akzeptanz für die geplanten und teils weitreichenden Änderungen zu sichern. Dabei wurde der kooperative und vertrauensvolle Ansatz der vergangenen Jahre, bei dem Behörden und Privatwirtschaft, Interessenvertretungen und beteiligte Ministerien gemeinsam und auf Augenhöhe die Weiterentwicklung von IT-Sicherheit diskutiert haben, als Beispiel für gesamtgesellschaftliches Handeln gegenüber einer wachsenden Bedrohung durch weltweit zunehmende Cyberangriffe wahrgenommen.

Dieser Ansatz wird mit der Novellierung des IT-Sicherheitsgesetzes in Teilen infrage gestellt. Weder wurde die im IT-SiG von 2015 vorgesehene Evaluierung der dort festgelegten Maßnahmen umgesetzt, noch scheint der aktuelle „Stellungnahmeprozess“ angesichts der Vielzahl kontroverser Regelungstatbestände geeignet, notwendige Abwägungen der Verhältnismäßigkeit einzelner Maßnahmen sicherstellen zu können. Darüber hinaus werden mit einzelnen Regelungen bewusst nationale Regelungen ohne europäisches Pendant verfolgt. Dies könnte Wettbewerbsnachteile für den Standort Deutschland nach sich ziehen oder, im ungünstigsten Fall, zu einer nachträglich notwendig werdenden Harmonisierung mit der auf europäischer Ebene maßgeblichen Netzwerk- und Informationssicherheits-Richtlinie (NIS-RL) führen.

Inhaltlich erweitert der Gesetzentwurf den bestehenden Ordnungsrahmen teilweise erheblich. Neben der Aufnahme neuer KRITIS-Sektoren und der Ausweitung der Befugnisse des Bundesamtes für Sicherheit in der Informationstechnik (BSI), z. B. für aktive Detektion von Sicherheitslücken („Portscans“), steht insbesondere die Ausweitung der Pflichten für Betreiber Kritischer Infrastrukturen – hier die Verpflichtung zur Detektion von Schadprogrammen - im Fokus des Gesetzgebers.

Auch eine massive Erhöhung möglicher Bußgelder sieht der Gesetzentwurf vor, um „Wertungswidersprüche bei Verstößen gegen die DSGVO und die NIS-Richtlinie zu beheben“.

Die Deutsche Krankenhausgesellschaft setzt sich seit vielen Jahren aktiv für die Verbesserung der Informationssicherheit in den deutschen Krankenhäusern ein. Neben dem Engagement im Rahmen des „Umsetzungsplans Kritische Infrastrukturen (UP KRITIS)“ steht vor allem die Veröffentlichung und Weiterentwicklung des sog. „Branchenspezifischen Sicherheitsstandards (B3S)“ im Mittelpunkt der Aktivitäten.

Informationssicherheit als ein Grundpfeiler für Digitalisierung im Gesundheitswesen bildet gemeinsam mit dem Datenschutz das Fundament für eine sichere und vertrauensvolle Nutzung digitaler Dienste im medizinischen Umfeld, insbesondere in den Krankenhäusern. Informationssicherheit ist letztlich immer auch Patientensicherheit. Diesem Umstand tragen Änderungen im SGB V Rechnung, nach denen künftig alle Krankenhäuser in Deutschland Maßnahmen zum Schutz ihrer informationstechnischen Systeme vorhalten müssen.

Die Position der Krankenhäuser zu einzelnen Regelungen sind dem Besonderen Teil zu entnehmen.

Besonderer Teil

Artikel 1

Änderung des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSIG)

Zu Artikel 1 Nummer 12 Buchstabe b (§ 8a Absatz 1a BSIG – neu)
Verpflichtung zur Vorhaltung von Systemen zur Angriffserkennung sowie Protokollierung entsprechender Information

Beabsichtigte Neuregelung

Mit § 8a Absatz 1a werden ausweislich der amtlichen Begründung die Betreiber kritischer Infrastrukturen verpflichtet, Systeme zur Angriffserkennung einzurichten.

Stellungnahme

Die Krankenhäuser schließen sich den Stellungnahmen des Bundesrates (BR-Drucksache 16/21) und des UP Kritis an, dass angesichts der administrativen und finanziellen Aufwände für Archivierung und Speicherplatz die Fristen zur Umsetzung unangemessen sind.

Als Systeme zur Angriffserkennung (Intrusion Detection Systeme – IDS) werden teils komplexe Systeme zur Erkennung von Angriffen und damit zum Schutz vor Missbrauch bezeichnet, deren Ziel aus Sicht des BSI darin besteht, *„aus allen im Überwachungsbereich stattfindenden Ereignissen diejenigen herauszufiltern, die auf Angriffe, Missbrauchsversuche oder Sicherheitsverletzungen hindeuten, um diese anschließend vertieft zu untersuchen. Ereignisse sollen dabei zeitnah erkannt und gemeldet werden. Intrusion-Detection ist als Prozess zu verstehen und bedarf einer geeigneten organisatorischen Einbindung sowie der technischen Unterstützung durch geeignete Werkzeuge.“*[1]

Zur Detektion von Angriffen kommen dabei gemäß BSI folgende Methoden zur Anwendung:

- Erkennung von Angriffsmustern
- Anomalieerkennung
    - durch Protokollanalyse
    - auf Basis statistischer Daten
    - auf Basis von Künstlicher Intelligenz

[1] BSI-Leitfaden zur Einführung von Intrusion-Detection-Systemen, abgerufen am 06.12.2020 unter https://www.bsi.bund.de/DE/Publikationen/Studien/IDS02/gr1_htm.html

  - auf Basis von Honeypots
- Korrelation von Ereignisdaten

Die genannten Methoden machen deutlich, dass es sich hierbei um wesentlich höhere Anforderungen handelt, als gemeinhin mit einer „Firewall“ verbunden werden. Neben entsprechender (Echtzeit-)Analyse des Netzwerkverkehrs, von Protokolldaten oder (intelligenter) Verknüpfung verschiedener Ereignisdaten kommt selbst die Einrichtung sogenannter Honeypots – also vermeintliche Echtsysteme, die potenziellen Angreifern ein lohnendes Ziel versprechen, um diese anzulocken und eine Angriffserkennung in einer kontrollierten Umgebung zu erleichtern – zum Einsatz.

Die Verpflichtung zur Einrichtung entsprechender Systeme besteht ab dem 01.01.2022. Somit bleibt voraussichtlich maximal ein Jahr zur Vorbereitung, um diese teils erheblich komplexen Anforderungen umzusetzen, die nicht allein im Bereich der Investitionen, sondern insbesondere bei „Betrieb“, „Personal“ und „Organisation“ ambitioniert sind. Neben der Einführung von geeigneter Hard- und Software ist auch der Aufbau entsprechender Monitoring-, Detektions-, Analyse-, Alarmierungs- und Reaktionsprozesse notwendig. Diese Aufgaben werden üblicherweise durch sog. Security Operation Center (SOC) wahrgenommen. Hierbei handelt es sich faktisch um den Aufbau von hochspezialisierten Teams, die 24/7 tätig sind. Für den Bereich des Gesundheitswesens – hier insbesondere die Krankenhäuser – besteht aktuell aufgrund der Covid-19-Pandemie sowie der massiven Digitalisierungsbestrebungen im Kontext der Telematikinfrastruktur, die seitens des BSI gesondert begleitet wird, ein erheblicher Handlungsdruck, der zu einer Überforderung der Krankenhäuser, die als kritische Infrastrukturen gelten, in diesem Bereich führen könnte. IDS sind bisher kein Gegenstand des branchenspezifischen Sicherheitsstandards. Auch wenn dies für die anstehende Überarbeitung berücksichtigt wird, halten zum gegenwärtigen Zeitpunkt selbst diejenigen Krankenhäuser, die entsprechende Maßnahmen zur Verbesserung der IT-Sicherheit umsetzen, ein IDS in der Regel nicht vor. Zudem bleibt die konkrete Ausgestaltung offen. Hier muss die Regelung auf IT-technische Minimalanforderungen begrenzt sein.

Änderungsvorschlag

Es ist eine realistische Übergangsfrist von mindestens zwei Jahren für die grundsätzliche Einführung von Systemen zur Angriffserkennung notwendig. Wenn es Branchen gibt, in denen entsprechende Systeme schon heute zum Stand der Technik zählen, könnte alternativ auch der Umsetzungszeitpunkt des Einsatzes von IDS in der Verordnung nach § 10 Abs. 5 BSIG branchenspezifisch geregelt werden und dabei die in der Gesetzesbegründung bereits angesprochenen unterschiedlichen Voraussetzungen in den einzelnen Branchen und Sektoren berücksichtigt werden.

Zu Artikel 1 Nummer 22 (§ 14 BSIG – neu)
Bußgeldvorschriften

Beabsichtigte Neuregelung

Aufgrund von Fragen der Zuständigkeit bei der Festlegung eines Strafmaßes im Falle einer Zuwiderhandlung gegen die im Gesetzentwurf enthaltenen Vorgaben werden Verstöße als Ordnungswidrigkeit geahndet, die jedoch mit Blick auf die Höhe des Strafmaßes (bis zu 20 Mio. EUR bei vorsätzlichem, bis zu 10 Mio. EUR bei fahrlässigem Handeln) dem europäischen Bußgeldrahmen der DSGVO entsprechen.

Stellungnahme

Die Krankenhäuser schließen sich der Stellungnahme des Bundesrates (BR-Drucksache 16/21) an, dass die Erhöhung der Bußgelder für Krankenhäuser und Universitätskliniken unverhältnismäßig und nicht tragbar ist.

Die Angleichung des Strafmaßes an den europäischen Bußgeldrahmen zur DSGVO war erwartet worden und das vorgeschlagene abgestufte Sanktionsmaß wird dabei als grundsätzlich sachgerecht angesehen. Allerdings erscheint die Erhöhung um das bis zu 200-fache des jetzigen Sanktionsmaßes (von derzeit 100.000 EUR auf bis zu 20 Mio. EUR) unverhältnismäßig und ist zu streichen. Der Erfüllungsaufwand für die Wirtschaft sollte gemäß der kürzlich durchgeführten Erhebung des Statistischen Bundesamts in den Sektoren der Kritischen Infrastrukturen beziffert werden.

Änderungsvorschlag

§ 14 Absatz 5 BSIG – neu wird wie folgt geändert:

(5) Die Ordnungswidrigkeit kann in den Fällen des Absatzes 2 Nummer 1 Buch-stabe a mit einer Geldbuße bis zu zwei Millionen Euro sowie in den Fällen des Absatzes 1 und des Absatzes 2 Nummer 2 und 3 mit einer Geldbuße bis zu einer Million Euro geahndet werden. Die Ordnungswidrigkeit kann in den Fällen des Absatzes 2 Nummer 1 Buch-stabe c, Nummer 5 und 7 bis 11 und des Absatzes 4 mit einer Geld-buße bis zu fünf-hunderttausend Euro sowie in den Fällen des Absatzes 2 Nummer 1 Buchstabe b, Nummer 4 und 6 und des Absatzes 3 mit einer Geldbuße bis zu hundert-tausend Euro geahndet werden. ~~**In den Fällen des Satzes 1 ist § 30 Absatz 2 Satz 3 des Gesetzes über Ordnungswidrigkeiten anzuwenden.**~~

Weiterer gesetzlicher Handlungsbedarf

Für den Gesundheitsbereich sind inzwischen eine Reihe von spezialgesetzlichen Regelungen zur Verbesserung der IT-Sicherheit u. a. im fünften Buch Sozialgesetzbuch aufgenommen worden (vgl. § 75c SGB V).

Im Zuge der Digitalisierung der Krankenhäuser hat das Bundesministerium für Gesundheit (BMG) eine Förderung, z. B. für Vorhaben zur Verbesserung der IT-Sicherheit in Krankenhäusern, über den so genannten Krankenhaus-Zukunftsfonds vorgesehen, dabei jedoch Krankenhäuser als Betreiber Kritischer Infrastrukturen explizit von dieser Fördermöglichkeit ausgenommen. Zur Begründung wird ausgeführt, dass diese nach dem so genannten Krankenhaus-Strukturfonds förderfähig wären und eine Doppelförderung ausgeschlossen werden müsse.

Mit dem Krankenhaus-Zukunftsfonds hat der Gesetzgeber einen Webfehler des Krankenhaus-Strukturfonds bereinigt, infolge dessen sich dieser Fonds als völlig dysfunktional in Bezug auf Maßnahmen für KRITIS-Betreiber herausgestellt hatte. Die bisher erforderliche Einvernehmensherstellung mit den gesetzlichen Krankenkassen wurde auf eine Benehmensherstellung reduziert. Bundesweit haben nach aktuellem Stand lediglich vier Krankenhäuser Fördermittel aus dem Krankenhaus-Strukturfonds erhalten, da in den meisten Fällen beantragte Mittel seitens der Krankenkassen mit deren Veto-Recht verhindert wurden.

In der aktuellen Covid-19-Pandemie wird der gesamtgesellschaftliche Wert der Krankenhäuser für die Gesundheitsversorgung deutlich. Ausgerechnet die Kliniken, die bereits gesetzlich dazu verpflichtet sind, hohe Anforderungen an die IT-Sicherheit ihrer informationstechnischen Systeme umzusetzen, werden jedoch seitens des BMG explizit von einer dringend benötigten Förderung dieser Maßnahmen ausgeschlossen. Dies widerspricht den Zielen der Vorsorgegesetzgebung und bestraft am Ende diejenigen Kliniken finanziell, die gemäß den Vorgaben der BSI-KritisV gesamtgesellschaftlich relevant sind. Es sollte ressortübergreifend sichergestellt werden, dass im Zuge von Gesetzgebungsverfahren keine solchen Fehlentwicklungen entstehen, die dem Ziel, die IT-Sicherheit zu verbessern und Cyberangriffe zu vermeiden, aktiv entgegenstehen. Noch befinden sich einige Gesetzgebungsverfahren aus dem BMG im parlamentarischen Prozess, sodass hier Fehlentwicklungen entgegengewirkt werden sollte.

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
19(4)745

VATM e. V. • Frankenwerft 35 • 50667 Köln

Vorab per E-Mail: CI1@bmi.bund.de
Bundesministerium des Inneren,
für Bau und Heimat
Abteilung Cyber- und Informationssicherheit
Alt-Moabit 140
10557 Berlin

Ansprechpartner	E-Mail	Fax	Telefon	Datum
Iris Nolte	in@vatm.de	0221 3767726	0221 3767727	13.01.2021

Entwurf eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (Zweites IT-Sicherheitsgesetz – IT-SiG 2.0)

Sehr geehrte Damen und Herren,

am 16.12.2020 hat die Bundesregierung einen Entwurf des „Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme („IT-Sicherheitsgesetz 2.0“) beschlossen. Der VATM hat bereits gemeinsam mit den Verbänden BREKO und BUGLAS bezüglich eines vorläufigen BMI-Entwurfs Stellung genommen. Aufgrund des Verfahrensablaufs, welches durch das BMI vorgegeben wurde, war eine ordentliche Beteiligung der Verbände innerhalb der Frist von einem Tag nach Veröffentlichung des letzten – aber erneut deutlich abgeänderten – Entwurfs nicht möglich. Der VATM möchte daher die Gelegenheit nutzen, auf Basis des Kabinettsbeschlusses einige weitere Punkte aufzuführen, die aufgrund der knappen Frist von VATM-Seite nicht mehr innerhalb der ersten Stellungnahme zur Diskussion gestellt werden konnten. Wir gehen davon aus, dass die von uns vorgetragenen Argumente noch ausreichend Berücksichtigung finden.

Der VATM begrüßt und unterstützt das Ziel, die Sicherheit informationstechnischer Systeme zu erhöhen. Unsere Mitgliedsunternehmen arbeiten intensiv an der Erreichung dieses Ziels. Der Entwurf des IT-Sicherheitsgesetzes 2.0 ist aus unserer Sicht aber nur in Teilen dazu geeignet, das Ziel sachgerecht und effizient zu erfüllen. Für die TK-Unternehmen, die die Basis für die Zukunftsfähigkeit der deutschen Wirtschaft bereitstellen, sind neue Pflichten vorgesehen, die zu großen Belastungen führen und über die Regelungen in §§ 109/109a TKG hinausgehen. Der Entwurf birgt Unklarheiten, die beseitigt werden müssen, um das Ziel der erhöhten Sicherheit erreichen zu können.

Ebenfalls ist es im Sinne der europäischen Harmonisierung wünschenswert, dass einer nationalen Fragmentierung entgegengewirkt wird und möglichst einheitliche Lösungen gesucht werden. Die „5G-Toolbox“ der EU-Kommission[1] bietet hier gute Ansatzpunkte, die so weit wie möglich im IT-SiG berücksichtigt werden sollten. Da viele Komponenten von TK-Unternehmen in ganz Europa eingesetzt werden, würde eine Harmonisierung zu einer deutlichen Effizienzsteigerung führen.

Darüber hinaus sollte das IT-Sicherheitsgesetz aber auch bereits neue 5G- und 6G-Technologien regulatorisch unterstützen.

I. Kein Aufbau von Wettbewerbsschranken

Das IT-Sicherheitsgesetz stellt hohe Anforderungen an die Verpflichteten. Neben den Betreibern kritischer Infrastrukturen wird der Kreis der Verpflichteten teilweise erweitert. Die Bedeutung der IT-Sicherheit nimmt in Zeiten der stetigen Digitalisierung immer weiter zu. Bei der Auferlegung der Anforderungen an die IT-Sicherheit darf der effektive Wettbewerb nicht aus den Augen verloren werden. Gesetzliche Regelungen wie das IT-Sicherheitsgesetz dürfen nicht als Wettbewerbs- und Markteintrittsschranken fungieren, indem sie Anforderungen aufstellen, die von kleineren und / oder neuen Marktteilnehmern nicht erbracht werden können. So finden sich zwar bereits im Rahmen der BSI-KritisV anhand bestimmter Schwellenwerte entsprechende Berücksichtigungen, die auch mit den Vorgaben des Post- und Telekommunikationssicherstellungsgesetz korrespondieren. Dieser Ansatz sollte auch für den nun neuen Kreis der Verpflichteten „Unternehmen im besonderen öffentlichen Interesse“ gewahrt werden.

Allgemein sollte aber auch überlegt werden, eine Abstufung der Verpflichtungen des IT-SiG 2.0 diesbezüglich in Betracht zu ziehen. Ein solches System könnte bspw. anhand von Größenkriterien beim Pflichtenumfang und / oder bei den Umsetzungsfristen differenzieren, um unter dem Gesichtspunkt von Wettbewerbschancen eine verhältnismäßige Umsetzung zu erreichen. Darüber hinaus könnte es auch sinnvoll sein, wenn insbesondere KMUs in die (vollen) Pflichten des IT-Sicherheitsgesetz mit der Zeit hineinwachsen können.

[1] Siehe hierzu auch den Workshop von ENISA und BEREC: https://berec.europa.eu/eng/events/berec_events_2020/258-joint-enisa-berec-workshop-on-5g-cybersecurity-toolbox-developments-and-ways-forward

VATM Verband der Anbieter von Telekommunikations- und Mehrwertdiensten e. V.
Frankenwerft 35 • 50667 Köln • Tel.: 0221 3767725 • Fax: 0221 3767726 • E-Mail: vatm@vatm.de

II. Bestandsdatenauskunft (§ 5c BSIG-E)

Gemäß § 5c BSIG-E soll das BSI künftig in den Kreis der berechtigten Stellen aufgenommen werden, die von den TK-Diensteanbietern eine Bestandsdatenauskunft im Wege des manuellen Auskunftsverfahrens nach § 113 Abs. 1 TKG anfordern können. Dies ist vor dem Hintergrund der Entscheidungen des Bundesverfassungsgerichts vom 27.05.2020 zum manuellen Auskunftsverfahren nicht unkritisch. Während es dem Bundesverfassungsgericht erkennbar darum geht, den Anwendungsbereich des manuellen Auskunftsverfahrens zu konkretisieren und zu beschränken, wird dieses durch § 5c BSIG-E für eine weitere Institution geöffnet, die zudem nicht unmittelbar den engen Bereichen des Polizeirechts oder der Landesverteidigung zuzurechnen ist.

Ergänzend zur gemeinsamen Verbände-Stellungnahme möchten wir zusätzlich zu unseren allgemeinen Bedenken ausführen:

Zunächst begrüßen wir die erst kurzfristig aufgenommene Entschädigungsregelung des neuen Absatzes 8, wonach den Verpflichteten eine entsprechende Aufwandsentschädigung nach § 23 und Anlage 3 JVEG zu gewähren ist.

Wir erachten es jedoch vor dem Hintergrund der Bundesverfassungsgerichts-Entscheidung vom Mai letzten Jahres für wichtig, dass ein ergänzender Absatz 9 eingefügt werden sollte. Hierin sollte klargestellt werden, dass die erhobenen Daten nach Behebung der Sicherheitsbeeinträchtigung unverzüglich zu löschen sind.

III. Neue Befugnisse des BSI (§ 7b-d BSIG-E)

Das BSI soll nach den Regelungen der § 7b-d BSIG-E neue Befugnisse erhalten. Insbesondere wird das BSI dazu ermächtigt, aktiv Sicherheitsrisiken aufzudecken und konkrete Anordnung zu erteilen, um Sicherheitsrisiken zu beseitigen. Aus Sicht des Gesetzeszwecks sehen wir diese neuen Befugnisse und die damit zugeordnete Rolle des BSI als „Gefahrenabwehrbehörde“ kritisch. Denn sie ermächtigen das BSI selbst in die IT-Sicherheit einzugreifen. Zur Abwehr der hierdurch potentiell entstehenden Gefahren wären weitere Konkretisierungen für eine tragbare Regelung erforderlich.

Nach § 7b BSIG-E wird das BSI dazu ermächtigt selbst Maßnahmen zu ergreifen, um Sicherheitsrisiken aufzudecken. Das BSI muss hier zumindest den Betreibern die nötige Transparenz

VATM Verband der Anbieter von Telekommunikations- und Mehrwertdiensten e. V.
Frankenwerft 35 • 50667 Köln • Tel.: 0221 3767725 • Fax: 0221 3767726 • E-Mail: vatm@vatm.de

verschaffen, indem es über den Beginn und die Beendigung der Durchführung der Maßnahmen informiert.

Nach § 7c und d BSIG-E soll das BSI zukünftig gegenüber TK-Diensteanbietern bzw. Telemedien-Anbietern auch befugt sein, konkrete Maßnahmen anzuordnen, um Gefahren für die IT-Sicherheit abzuwenden. Gem. § 7c Abs. 3 BSIG-E kann das BSI anordnen, den Datenverkehr an eine benannte Anschlusskennung umzuleiten. Hier sehen wir dringend weiteren Klarstellungsbedarf, da die Umleitung des Telekommunikationsverkehrs an Dritte eine Verletzung des Fernmeldegeheimnisses darstellt, die es besonders zu begründen gilt. § 7c Abs. 3 BSIG-E bedarf daher der weiteren Konkretisierung, die die Verletzung des Fernmeldegeheimnisses gebührend begründet.

Das BSI erlangt sowohl aus der Ermächtigung zur aktiven Aufdeckung von Sicherheitsrisiken als auch durch die Möglichkeit zur Anordnung konkreter Maßnahmen zu deren Behebung weitreichende Befugnisse, selbst in die IT-Sicherheit der Betreiber einzugreifen. Auch durch einen solchen Eingriff in die IT-Sicherheit können Gefahren entstehen, die geeignet sind, die IT-Infrastrukturen der Unternehmen erheblich zu beeinträchtigen. Dies kann bspw. auch in einem Ausfall der Systeme resultieren. Für die hierdurch entstehenden Schäden bedarf es daher ergänzend einer entsprechenden Kompensationsregelung zugunsten der Betreiber, wenn diese Schäden das Resultat einer, vom BSI vorgenommenen oder angeordneten Handlung sind.

IV. Sicherheit in der Informationstechnik kritischer Infrastrukturen (§ 8a BSIG-E)

Nach dem neuen § 8a Abs. 1a BSIG-E sollen Betreiber kritischer Infrastrukturen zukünftig verpflichtet werden, auch Systeme zur Angriffserkennung einzusetzen. Grundsätzlich unterstützen wir den Einsatz von Systemen zur Angriffserkennung, da diese einen wichtigen Beitrag zur IT-Sicherheit leisten können. Allerdings sehen wir eine allgemeine Verpflichtung im Lichte des Systems nach § 8a BSIG-E kritisch. Dieser ist gerade darauf ausgelegt, technische und organisatorische Maßnahmen nach dem jeweils erforderlichen Bedarfsfall auszuwählen und zu implementieren, um einen für diesen Fall zuverlässigen Schutz zu gewährleisten. Eine allgemeine Verpflichtung steht diesem System entgegen.

Darüber hinaus ist die Definition nach § 2 Abs. 9b BSIG-E hier auch zu unbestimmt, wodurch es bereits schwer sein wird zu bestimmen, ob die Betreiber die nötigen Anforderungen überhaupt erfüllt haben. Das BSI soll hierzu ermächtigt werden, durch Richtlinien die Anforderungen zu

VATM Verband der Anbieter von Telekommunikations- und Mehrwertdiensten e. V.
Frankenwerft 35 • 50667 Köln • Tel.: 0221 3767725 • Fax: 0221 3767726 • E-Mail: vatm@vatm.de

Präsidium: Martin Witt (Präsident), David Zimmer (Vizepräsident), Valentina Daiber, Michael Jungwirth,
Uwe Nickl, Karsten Rudloff, Rickmann von Platen, Norbert Westfal, Peter Zils • Geschäftsführer: Jürgen Grützner

konkretisieren. Die Erstellung und zukünftige Änderungen dieser Richtlinien sollten unter der Beteiligung der Unternehmen erfolgen.

Abschließend halten wir die Verpflichtung der Betreiber nach Abs. 3 S. 1, alle zwei Jahre die Erfüllung der Anforderungen nachzuweisen, für problematisch. Hier sollte ein längeres Zeitintervall, wie bspw. alle fünf Jahre, angesetzt werden.

V. Registrierung kritischer Infrastrukturen (§ 8b Abs. 3 BSIG-E)

Gem. § 8b Abs. 3 BSIG-E sollen Betreiber kritischer Infrastrukturen ihre Anlagen beim BSI registrieren. In dieser Regelung sehen wir im Bereich der Telekommunikationsanbieter erhebliche Probleme, die zu parallelen Strukturen zwischen der BNetzA und dem BSI führen können. Hier bedarf es unbedingt einer Klarstellung, um unnötige Doppelregulierungen und Zuständigkeitsfragen zu vermeiden.

VI. Herausgabe von Informationen (einschließlich personenbezogener Daten) (§ 8b Abs. 4a BSIG-E)

Gem. § 8b Abs. 4a BSIG-E besteht im Falle einer erheblichen Störung die Pflicht zur Herausgabe der notwendigen Informationen (einschließlich personenbezogener Daten) an das Bundesamt, die zur Bewältigung der Störung notwendig sind. Besonders mit Blick auf die Herausgabe personenbezogener Daten sehen wir diese Regelung äußerst kritisch und wünschen uns diesbezüglich weitere Klarstellungen.

VII. Sicherheit in der Informationstechnik bei Unternehmen im besonderen öffentlichen Interesse (§ 8f BSIG-E)

Der neue § 8f BSIG-E sieht für die „Unternehmen von besonderem öffentlichen Interesse“ insbesondere die Verpflichtung vor, eine Selbsterklärung zur IT-Sicherheit abzugeben. Der Zweck dieser Selbsterklärung ist für uns jedoch nicht nachvollziehbar. Ausgehend von der Definition des Begriffs der „Unternehmen von besonderem öffentlichen Interesse“ verstehen diese Unternehmen die Bedeutung der IT-Sicherheit selbst und werden sie aus eigenem Anreiz gewährleisten. Zudem scheinen einige Regelungen daran anzuknüpfen, die Wertschöpfung dieser Unternehmen aufgrund von Störungen nicht gefährden zu wollen und erlegen diesbezügliche Verpflichtungen

VATM Verband der Anbieter von Telekommunikations- und Mehrwertdiensten e. V.
Frankenwerft 35 • 50667 Köln • Tel.: 0221 3767725 • Fax: 0221 3767726 • E-Mail: vatm@vatm.de

Präsidium: Martin Witt (Präsident), David Zimmer (Vizepräsident), Valentina Daiber, Michael Jungwirth,
Uwe Nickl, Karsten Rudloff, Rickmann von Platen, Norbert Westfal, Peter Zils • Geschäftsführer: Jürgen Grützner

auf. Dieser Ansatz ist mit dem Telos des Gesetzes nur schwer vereinbar. Zumal auch hier wirtschaftlich agierende Unternehmen aus eigenem Anreiz Maßnahmen ergreifen werden, um ihre eigenen Wertschöpfungsprozesse nicht zu gefährden. Auch die weiteren Regelungen des § 8f BSIG-E bauen auf dem angeordneten Selbstbekenntnis zur IT-Sicherheit auf und führen zu hohem bürokratischem Aufwand, ohne dass der Nutzen hierzu ersichtlich ist. § 8f BSIG-E sollte daher gestrichen werden.

VIII. Zertifizierung (§ 9 BSIG)

Nach § 9 Abs. 4 S. 1 Nr. 2 i.V.m. Abs. 4a BSIG-E kann das BMI die Erteilung eines Zertifikats untersagen, wenn überwiegende öffentliche Interessen, insbesondere sicherheitspolitische Belange der Bundesrepublik Deutschland, der Erteilung entgegenstehen. Das technische Zertifizierungsverfahren, welches sich ausschließlich nach den telekommunikationsrechtlichen Bestimmungen zu richten hat, würde durch eine zusätzliche Überprüfung seitens des BMI um eine sicherheitspolitische Bewertung ergänzt. Unabhängig davon, dass hier eine unbedingt zu vermeidende Doppelprüfung im Raum steht, sollen rein technisch geprägte Zertifizierungsverfahren gerade aufgrund ihrer objektiven Kriterien zur Rechts- und Planungssicherheit beitragen. Mit einer politischen Bewertung, bei der erhebliche Bewertungsspielräume bestehen können, wird diese Rechts- und Planungssicherheit untergraben. Zudem kann sich durch eine zusätzliche (und vor allem sachfremde) Prüfung durch das BMI das Zertifizierungsverfahren erheblich verlängern. Besonders zweckfremd erscheint die Prüfung durch das BMI vor dem Hintergrund der Zertifizierung kritischer Komponenten, die daran anschließend eine erneute Überprüfung anhand sicherheitspolitischer Erwägungen durchlaufen müssen (siehe § 9b BSIG-E). Hiermit käme es praktisch zu einer erneuten Prüfung. Zudem ist dabei zu berücksichtigen, dass im Gegensatz zu dem Verfahren nach § 9b BSIG-E allein das BMI darüber entscheiden darf, ein Zertifikat aus sicherheitspolitischen Bedenken nicht zu erteilen.

Der Regelungsrahmen für die Erteilung eines Zertifikats sollte sich daher rein auf die technischen Fragestellungen begrenzen.

Ebenfalls sollte bedacht werden, dass die Hersteller selbst die Zertifizierungen beantragen, damit diese mit den zuständigen Behörden in die Klärung bestehender (Fach-)Fragen gehen können. Dies darf und sollte nicht über die Netzbetreiber abgehandelt werden. Ansonsten droht nicht nur ein unüberschaubarer bürokratischer Aufwand, sondern auch eine besondere Benachteiligung kleiner TK-Unternehmen, die diesen Aufwand nicht stemmen können.

VATM Verband der Anbieter von Telekommunikations- und Mehrwertdiensten e. V.
Frankenwerft 35 • 50667 Köln • Tel.: 0221 3767725 • Fax: 0221 3767726 • E-Mail: vatm@vatm.de

Darüber hinaus sollten im Lichte eines harmonisierten EU-Binnenmarkts Zertifizierungen anderer EU-Behörden anerkannt werden, ohne dass eine erneute Zertifizierung vom BSI erforderlich ist (One-Stop-Shop-Prinzip).

IX. Untersagung des Einsatzes kritischer Komponenten (§ 9b BSIG-E)

Es ist richtig, ausschließlich verlässliche Komponenten für den Einsatz in kritischen Infrastrukturen zuzulassen. Dieses Ziel wird auch nachdrücklich unterstützt und begrüßt. Dennoch sehen wir in den hierzu getroffenen Regelungen Verbesserungsmöglichkeiten, um das Ziel des sicheren Betriebs kritischer Infrastrukturen zu gewährleisten.

1. Definition „kritischer Komponenten“

Der Begriff der „kritischen Komponenten“ wird in § 2 Abs. 13 BSIG-E definiert. Während aus den früheren Gesetzesbegründungen hierzu noch hervorging, dass die Bestimmung der kritischen Komponenten sich ausschließlich nach den Vorgaben des TK-Sicherheitskatalogs und seiner Anlage 2 ergeben, ließe sich aus der derzeitigen Gesetzesformulierung auch der Schluss ziehen, dass kritische Komponenten auch durch andere Gesetzesvorschriften bestimmt werden können. Vor allem vor dem Hintergrund der Bewertungen durch das BMI und den beteiligten Ressorts im Rahmen der Prüfung nach § 9b Abs. 3 S. 1 BSIG-E bedarf es hier einer Klarstellung, damit sich die kritischen Komponenten abschließend allein aus den telekommunikationsrechtlichen Bestimmungen nach § 109 Abs. 6 TKG i.V.m. Anlage 2 TK-Sicherheitskatalog ergeben.

2. Garantieerklärung

Der neue § 9b BSIG-E möchte das Ziel der IT-Sicherheit im Zusammenhang mit dem Einsatz „kritischer Komponenten“ insbesondere mit der Abgabe einer Garantieerklärung (Vertrauenswürdigkeitserklärung) der Hersteller gegenüber den Betreibern kritischer Infrastrukturen erreichen. Der Entwurf beinhaltet hohe Anforderungen an die eingesetzten Komponenten und Hersteller. So sollen Hersteller versichern, dass und wie sie hinreichend sichergestellt haben, dass die von ihnen hergestellte „kritische Komponente über keine technischen Eigenschaften verfügen, die geeignet sind, missbräuchlich, insbesondere zu Zwecken von Sabotage, Spionage oder Terrorismus auf die Sicherheit, Integrität, Verfügbarkeit oder Funktionsfähigkeit der kritischen Infrastruktur, einwirken zu können“.

Konkrete Aussagen zu den Bestandteilen der Garantieerklärung lässt die Regelung allerdings vermissen. So ist es bspw. unklar, ob die Zertifikate der Hersteller bereits Bestandteil der

VATM Verband der Anbieter von Telekommunikations- und Mehrwertdiensten e. V.
Frankenwerft 35 • 50667 Köln • Tel.: 0221 3767725 • Fax: 0221 3767726 • E-Mail: vatm@vatm.de

Erklärung sind oder erst später beizubringen sind. Das Gesetz verweist zum Inhalt der Garantieerklärung auf eine – zu einem späteren Zeitpunkt zu erlassene – Allgemeinverfügung des BMI. Hier sollte eine Klarstellung aufgenommen werden. Aus Gründen der Planungs- und Rechtssicherheit für die betroffenen Unternehmen sollte der Mindestinhalt (z.B. inhaltlich entsprechend der Vertrauenswürdigkeitserklärung betreffend die Logistikkette gemäß Ziffer 3 der Anlage 2 TK-Sicherheitskatalog) bereits in § 9b BSIG-E enthalten sein, der dann anschließend durch eine Allgemeinverfügung weiter konkretisiert werden kann. Die anschließende Allgemeinverfügung muss dann auch den Grundsätzen der Bestimmtheit, Verhältnismäßigkeit und dem Übermaßverbot (vgl. §§ 35 ff VwVfG) genügen.

Weiterhin sollte im Rahmen der Erstellung und ggf. Überarbeitung der Allgemeinverfügung des BMI den beteiligten Stakeholdern hier die Möglichkeit der Anhörung gegeben werden.

3. Prüfprozess

Der Einsatz kritischer Komponenten ist mit einer Prüfung des BMI und den „beteiligten Ressorts“ verbunden. Ein vorheriger Einsatz ist nicht gestattet. Nach § 9b Abs. 3 BSIG-E erfolgt diese Prüfung innerhalb eines Monats. In der Vorschrift wäre eine Klarstellung hilfreich, ob mit Übermittlung der Garantieerklärung an das BMI automatisch der Prüfprozess nach § 9b Abs. 3 BSIG-E eingeleitet wird. Weiterhin ist nach dem bisherigen Gesetzeswortlaut die Frist von einem Monat als nicht verlängerbare Ausschlussfrist zu interpretieren und nach Ablauf selbiger von einer Genehmigung betreffend den Einsatz der Komponenten auszugehen. Aus Gründen der Rechtsklarheit sollte hierzu jedoch eine Klarstellung in einem ergänzenden Satz erfolgen.

Weiterhin sehen wir auch die Notwendigkeit einer Konkretisierung des Prüfverfahrens. Nach § 9b Abs. 3 sind hieran das BMI unter Abstimmung mit den „beteiligten Ressorts“ beteiligt. Leider finden sich weder im Rechtstext noch in den Begründungen entsprechende Ausführungen, welche Ressorts konkret beteiligt sind oder sich beteiligen können. Die Nennung des BMWi erscheint in der Begründung nur beispielhaft erwähnt worden zu sein. Da die Prüfung zu einer Verzögerung des Einsatzes „kritischer Komponenten“ führt, bedarf es hier eines vorab definierten Kreises der beteiligten Behörden, die diese Entscheidung treffen werden. Die Betreiber kritischer Infrastrukturen dürfen nicht zum Spielball eines behörden-internen „Zuständigkeitsgerangel“ werden. Zudem ist zu bedenken, dass der verzögerte Einsatz „kritischer Komponenten“ ebenfalls eine Gefahr für die IT-Sicherheit darstellen kann, die das Gesetz gerade verhindern möchte.

Neben einer Konkretisierung der am Prüfprozess beteiligten Ressorts sehen wir auch das Erfordernis einer Konkretisierung der Prüfungskriterien selbst. So ist nach § 9b Abs. 3 BSIG-E die

VATM Verband der Anbieter von Telekommunikations- und Mehrwertdiensten e. V.
Frankenwerft 35 • 50667 Köln • Tel.: 0221 3767725 • Fax: 0221 3767726 • E-Mail: vatm@vatm.de

Prüfung anhand „überwiegender öffentlicher Interessen, insbesondere sicherheitspolitische Belange der Bundesrepublik Deutschland“ vorzunehmen.

Der Auf- und Ausbau von Telekommunikationsnetzen, insbesondere der bereits laufende Ausbau des 5G-Netzes, verlangt einen hohen Investitionsaufwand. Auch die Politik und die Kunden erwarten von den Netzbetreibern diese Investitionen. Im Gegenzug muss den Unternehmen eine entsprechende Planungssicherheit zugesprochen werden. Insofern bedürfen die Kriterien der Vertraulichkeitsprüfung einer Konkretisierung, die es den Unternehmen erlaubt, hier eine Risikobewertung bereits im Vorfeld vorzunehmen. Der Bedarf konkreter Bewertungskriterien ist darüber hinaus auch deshalb zwingend, da durch den inländisch politischen Wandel oder personelle Änderungen in den Ressorts die Gefahr einer willkürlichen Entscheidung verstärkt werden, wenn es an diesen Kriterien fehlt. Bei der Konkretisierung der Bewertungskriterien sollte dann schließlich darauf geachtet werden, dass politische Erwägungen sich einzig auf die Schutzziele des IT-Sicherheitsgesetzes wie die Gefahren für die Verfügbarkeit, Integrität, Vertraulichkeit und Authentizität beziehen dürfen. Ziel des Gesetzes ist es nicht, die politische Lage anderer Staaten „durch die Hintertür“ zu sanktionieren, indem Hersteller aus diesen Ländern als nicht vertrauenswürdig angesehen werden. Dies ist nicht der Zweck des IT-Sicherheitsgesetzes und würde andernfalls die Betreiber kritischer Infrastrukturen unverhältnismäßig belasten, wenn diesen bspw. der Einsatz kritischer Infrastrukturen aufgrund von politischen Erwägungen untersagt werden, die außerhalb des Regelungsziels des IT-Sicherheitsgesetzes stehen.

4. Rechtsfolge

Gemäß § 9b Abs.4 BSIG-E kann das BMI den weiteren Betrieb einer „kritischen Komponente“ gegenüber dem Betreiber einer kritischen Infrastruktur untersagen, wenn der Hersteller der „kritischen Komponente“ sich als nicht vertrauenswürdig im Sinne des Abs. 5 erwiesen hat, also insbesondere gegen die dem Betreiber der kritischen Infrastruktur gegenüber abzugebende Garantieerklärung verstoßen hat. Das BMI hat seine Entscheidung im Einvernehmen mit den beteiligten Ressorts zu treffen.

a) Nachträgliche Untersagung

Die nachträgliche Untersagung bereits verbauter Komponenten stellt einen erheblichen Eingriff in die Berufs- und Eigentumsfreiheit der beteiligten Unternehmen dar. Ein solcher Eingriff bedarf einer entsprechenden Rechtfertigung. Die Notwendigkeit eines solchen Eingriffs ergibt sich jedoch nicht aus der derzeitigen Regelung. Gerade mit dem vorgeschalteten Prüfungsprozess, bei dem nicht nur die technische Zuverlässigkeit der Komponenten bescheinigt, sondern auch

VATM Verband der Anbieter von Telekommunikations- und Mehrwertdiensten e. V.
Frankenwerft 35 • 50667 Köln • Tel.: 0221 3767725 • Fax: 0221 3767726 • E-Mail: vatm@vatm.de

Präsidium: Martin Witt (Präsident), David Zimmer (Vizepräsident), Valentina Daiber, Michael Jungwirth,
Uwe Nickl, Karsten Rudloff, Rickmann von Platen, Norbert Westfal, Peter Zils • Geschäftsführer: Jürgen Grützner

zusätzlich die Prüfung nach Abs. 3 durchlaufen wird, lassen einer nachträglichen Untersagung wenig Raum.

Die Möglichkeit einer jederzeitigen – und von dem Betreiber nicht kontrollierbaren oder gar kalkulierbaren – Untersagung, sind vor dem Hintergrund der Rechtssicherheit ein unverhältnismäßiges Mittel. Darüber hinaus fehlt es dem Gesetz auch an entsprechenden Regelungen, die den Rückbau der betroffenen Komponenten regelt. Aufgrund von teils sehr komplexen und / oder quantitativen Faktoren wäre ein Rückbau nach Anordnung der Untersagung rein operativ schwer möglich. Wir sehen die Rechtsfolge der Untersagung daher insgesamt als unverhältnismäßiges Mittel an. § 9 Abs. 4 BSIG-E sollte daher gestrichen werden. Doch selbst wenn an dieser Regelung festgehalten wird, bedarf es unbedingt ergänzender Vorschriften, die es den Unternehmen ermöglichen, die Rechtsfolge in einer angemessenen Zeit umzusetzen.

Die Möglichkeit der nachträglichen Untersagung und ihrer Folgen müssen vor allem auch vor dem Hintergrund der ergänzenden Regelungen der Absätze 6 und 7 betrachtet werden. Danach können auch weitere Komponenten des Herstellers im Falle einer fehlenden Vertrauenswürdigkeit untersagt werden. Unter den bereits oben benannten Aspekten der Planungs- und Rechtssicherheit der Betreiber halten wir diese erweiterte Rechtsfolge für äußerst problematisch. So könnte bereits im Falle des Absatz 6 der erstmalige Verstoß ausreichen, der zur weiteren Untersagung führt. Darüber hinaus fehlt es der Regelung auch an generellen Verfahrensregelungen. Während die Untersagung einer Komponente im direkten Verfahren mit einem Betreiber erfolgt, greift die nachträgliche Untersagung nach den Absätzen 6 und 7 wohl unabhängig von bestimmten Betreibern. Hier stellt sich dann die Frage, woher die Betreiber die nötigen Informationen erhalten, wenn die Entscheidung über die weitere Untersagung „kritischer Komponenten“ nicht innerhalb ihres eigenen Verfahrens getroffen wird. Darüber hinaus bedürfte eine solche Regelung unbedingt entsprechender Vorschriften, die die Umsetzungszeit regeln. Wenn hiermit ggf. betreiber-übergreifend die kritischen Komponenten von Herstellern untersagt werden, muss den Betreibern für die Umsetzung entsprechend Zeit eingeräumt werden. Andernfalls drohen durch diese Vorgaben erhebliche Gefahren für die IT-Sicherheit, wenn alle betroffenen Betreiber innerhalb kürzester Zeit entsprechende Alternativlösungen abwägen und implementieren müssten.

Wir möchten daher darauf hinweisen, dass diese Bedenken im Rahmen einer nachträglichen Untersagung berücksichtigt werden müssen. Zu begrüßen ist, dass der Kabinettsbeschluss jedenfalls die Beteiligung der betroffenen Ressorts in Absatz 7 ergänzt hat.

VATM Verband der Anbieter von Telekommunikations- und Mehrwertdiensten e. V.
Frankenwerft 35 • 50667 Köln • Tel.: 0221 3767725 • Fax: 0221 3767726 • E-Mail: vatm@vatm.de

b) Recht auf rechtliches Gehör

Bevor das BMI mit der Zustimmung der beteiligten Ressorts den Einsatz von kritischen Komponenten aufgrund fehlender Vertrauenswürdigkeit des Herstellers (nachträglich) untersagen darf, ist es zwingend erforderlich, dass die Betroffenen angehört werden. Dies gebietet das grundrechtlich geschützte Recht auf rechtliches Gehör und ist in Anbetracht der drastischen Folgen einer – vor allem nachträglichen – Untersagung nach dem Verhältnismäßigkeitsgrundsatz für die Betreiber geboten.

c) Regress gegenüber dem Staat

§9b BSIG-E führt zu erheblichen Rechts- und Planungsunsicherheiten bei den Betreibern kritischer Infrastrukturen. Wie gezeigt fehlt es an nachprüfbaren Kriterien woran das BMI und die beteiligten Ressorts die fehlende Vertrauenswürdigkeit der Hersteller festmachen können und dürfen. Ergänzend fehlt es an konkretisierten Instrumenten der Betreiber sich vor der Entscheidung im Wege des einstweiligen Rechtsschutzes zu schützen. Die Folgen für die Betreiber, aber auch für die Sicherheit der Netze aufgrund fehlender Umsetzungszeiten sind groß. Es besteht die Gefahr, dass Hersteller aus unberechtigten Gründen als nicht vertrauenswürdig eingestuft werden und den Betreibern hieraus erhebliche Schäden entstehen können. Sofern es an entsprechenden Schutzinstrumenten fehlt, die den Schadenseintritt verhindern, muss der Staat entsprechend haftbar gemacht werden können.

d) Bestandsschutz

Abschließend sollte auch klargestellt werden, dass die Verpflichtungen keine Auswirkungen auf bereits langjährig erprobte und zuverlässig eingesetzte Komponenten haben. Es bedarf eines Schutzes der derzeitigen Bestandsnetze, weshalb sich die Pflichten nur auf Komponenten beziehen dürfen, die seit Inkrafttreten des neuen Gesetzes (bzw. nach Geltung der Verordnung zur Konkretisierung kritischer Komponenten) eingebaut wurden. Andernfalls droht den Verpflichteten hier ein erheblicher Investitionsaufwand, der bei der damaligen Auswahl der entsprechenden Komponenten nicht berücksichtigt werden konnte. Dies kann nicht nur zu erheblichen Investitionen führen, sondern beeinflusst auch direkt den zukünftigen Ausbau der Infrastrukturnetze.

VATM Verband der Anbieter von Telekommunikations- und Mehrwertdiensten e. V.
Frankenwerft 35 • 50667 Köln • Tel.: 0221 3767725 • Fax: 0221 3767726 • E-Mail: vatm@vatm.de

X. Offenlegungspflicht (§ 10 Abs. 6 BSIG-E)

Der neue § 10 Abs. 6 BSIG-E sieht vor, dass das BMI unter Beteiligung von Verbänden und des BMWi durch Rechtsverordnung die Offenlegung von Schnittstellen und die Einhaltung etablierter technischer Standards bestimmen kann. Eine derart allgemeine Anordnungsbefugnis zur Offenlegung von Schnittstellen, Einhaltung etablierter technischer Standards und Interoperabilität halten wir aus europarechtlichen Gründen für äußerst problematisch. Noch dazu, weil generell von Komponenten und Prozessen gesprochen wird, anstatt den Fokus auf kritische Komponenten zu begrenzen und keine Konkretisierung „etablierter" technischer Standards erfolgt. Hiermit wird das BMI ermächtigt, Komponenten über die „kritischen Komponenten nach § 2 Abs. 13 BSIG-E" hinaus zu regulieren, ohne dass der Zweck dieser Ermächtigung erkennbar ist. Die Offenlegung von Schnittstellen dient jedenfalls nicht der Erreichung der Schutzziele des IT-SiG, also der Gewährleistung der Cyber- und Informationssicherheit. Im Gegenteil: Durch die Offenlegung wird ein Sicherheitsrisiko dergestalt geschaffen, dass sensible, für den Schutz der Netzwerke relevante Informationen, in die Hände böswilliger Akteure fallen könnten. § 10 Abs. 6 sollte damit ersatzlos gestrichen werden.

XI. Bußgelder (§ 14 BSIG-E)

Abschließend möchten wir erneut darauf hinweisen, dass die Bußgelder aufgrund des Verweises auf § 30 Absatz 2 Satz 3 OWiG unverhältnismäßig hoch ausfallen können. Der Verweis auf das OWiG sollte daher unbedingt gestrichen werden.

Wir bitten um die Berücksichtigung der aufgezeigten Erwägungen und stehen für Rückfragen gerne zur Verfügung.

VATM Verband der Anbieter von Telekommunikations- und Mehrwertdiensten e. V.
Frankenwerft 35 • 50667 Köln • Tel.: 0221 3767725 • Fax: 0221 3767726 • E-Mail: vatm@vatm.de

VERBAND DER INTERNETWIRTSCHAFT E.V.

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
19(4)747

Ergänzende Anmerkungen und Stellungnahme zum Referentenentwurf des Bundesministeriums des Innern für Bau und Heimat eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (Zweites IT-Sicherheitsgesetz – IT-SiG 2.0) (Stand 9.12.2020)

Berlin 10. Dezember 2020

Am 9. Dezember 2020 hat eco – Verband der Internetwirtschaft e.V. den am 1. Dezember desselben Jahres veröffentlichten Diskussionsentwurf des Bundesministeriums des Innern für Bau und Heimat (BMI) zum Zweiten Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (Zweites IT-Sicherheitsgesetz – nachfolgend IT-SiG 2.0) kommentiert und hierzu eine umfangreiche Stellungnahme eingereicht.

Am selben Tag übermittelte das BMI einen überarbeiteten Referentenentwurf zur Verbändebeteiligung gem. § 47 (3) der gemeinsamen Geschäftsordnung der Bundesministerien mit Frist zum 10. Dezember 2020.

In Anbetracht der eingeräumten Frist von lediglich einem Tag zur Beteiligung ist eine der Bedeutung und Auswirkungen des IT-SiG 2.0 angemessene und umfassende Würdigung des Gesetzesentwurfs nur sehr eingeschränkt möglich.

eco verweist unbeschadet etwaiger Änderungen in dem nun vorliegenden Referentenentwurf des IT-SiG 2.0 auf seine umfassende Kommentierung.

Ergänzend dazu macht eco noch folgende Anmerkungen zu dem vorliegenden Referentenentwurf. Er beschränkt sich dabei auf Aspekte, die durch den nunmehr vorliegenden Referentenentwurf geändert wurden. Diese Kommentierung ist als Ergänzung zur Stellungnahme über den Diskussionsentwurf zu lesen, die er im Übrigen und sofern hier nicht anders dargelegt aufrechterhält:

Zu Artikel 1 Nr. 1 f

Ergänzend zu den Anmerkungen zum Diskussionsentwurf möchte eco festhalten, dass die Neufassung des § 2 (13) BSI-G-neu nunmehr die Möglichkeit zur Feststellung kritischer Funktionen vorsieht, aus denen wiederum kritische Komponenten abgeleitet werden können.

Die vorliegende Formulierung lässt leider keinen Rückschluss darauf zu, wie genau sich diese kritischen Funktionen aus einem Gesetz ableiten lassen sollen. Auch die Begründung gibt hierzu leider keinerlei sachdienlichen Hinweise. Infolgedessen bleibt unklar, wie sich aus kritischen Funktionen wiederum kritische Komponenten ableiten lassen. Insgesamt erweckt diese Formulierung den Eindruck, dass damit der Vorbehalt, kritische

Komponenten ausschließlich gesetzlich zu definieren, ausgehebelt werden soll. In der Konsequenz ist auch die Umformulierung des Absatzes zur gesetzlichen Grundlage für die Festlegung kritischer Komponenten problematisch.

eco erneuert seine Kritik an dem Gesetzentwurf: Für kritische Komponenten muss eine eindeutige gesetzliche Grundlage bestehen. Eine abstrakte Ableitung aus Gesetzen oder Funktionen, die wiederum aus weiteren Gesetzen abgeleitet sind, ist unkonkret und daher abzulehnen.

Die im Vergleich zum Diskussionsentwurf vom 1. Dezember vorgenommenen Streichungen im § 2 (14) BSI-G-neu zur näheren Bestimmung von Unternehmen von besonderem öffentlichen Interesse sind nach Ansicht des eco ebenfalls als problematisch zu bewerten. Es wird der Eindruck erweckt, dass nicht, wie ursprünglich zu vermuten war, nur wenige ausgewählte Unternehmen von dieser Regelung betroffen sein werden, sondern, dass der Adressatenkreis der Norm deutlich weiter gefasst sein könnte. eco fordert den Gesetzgeber auf, die durch den vorliegenden Entwurf hervorgerufenen Unsicherheiten und Unklarheiten hinsichtlich des Anwendungsbereichs und des Adressatenkreises zu beseitigen und hierdurch Rechtssicherheit bei den betroffenen Unternehmen zu schaffen. Es sind normenklare, nachvollziehbare und verhältnismäßige Anforderungen an die Definition eines Unternehmens von besonderem öffentlichen Interesse zu formulieren.

Zu Artikel 1 Nr. 10

Die in §7c BSI-G-neu geschaffene Anordnungsbefugnis für das BSI begründet eine Doppelzuständigkeit für den Sektor der Telekommunikation für das BSI einerseits und die Bundesnetzagentur (BNetzA) andererseits aufgrund des Telekommunikationsgesetzes. Eine solche Doppelzuständigkeit wird von eco kritisch bewertet und abgelehnt.

Inakzeptabel erscheint zudem die mit dem Referentenentwurf hinzugekommene Auferlegung der Verantwortung zu Lasten der Telekommunikationsanbieter für Router, die deren Kunden käuflich erworben haben. Der Gesetzgeber lässt zwar in der Gesetzesbegründung erkennen, dass ihm bewusst ist, dass rechtlich ein Unterschied zwischen von Anbietern überlassenen Routern und von deren Kunden gekauften Geräten besteht, vgl. S. 77, zweiter Absatz. Gleichwohl will der Gesetzgeber die Verantwortung für die Kaufgeräte auch den TK-Anbietern zuweisen. Damit behandelt er ohne sachliche Rechtfertigung wesentlich Ungleiches gleich.

Zu Artikel 1 Nr. 12

Die gegenüber dem Diskussionsentwurf vorgesehene Verkürzung der Umsetzungsfrist für den Einsatz von Systemen zur Angriffserkennung ist mit einem Werktag deutlich kurz bemessen. Nach Ansicht des eco sollte die Frist zur Umsetzung und Implementierung mindestens 12 Monate betragen. Insbesondere auch, da davon auszugehen ist, dass sich aus der Verpflichtung zum Einsatz entsprechender Systeme weitere Fragestellungen zu den jeweils passenden Detektionssystemen und deren Integration in vorhandene Infrastrukturen ergeben. Unsere grundsätzliche Kritik an der Vorschrift hatten wir bereits in unserer Stellungnahme zum Diskussionsentwurf ausführlich dargelegt.

Zu Artikel 1 Nr. 17

eco möchte ergänzend zu seiner ausführlichen Kommentierung im Rahmen des Diskussionsentwurfs darauf hinweisen, dass die vorgenommene Verkürzung der Frist zur Vorlage von Informationen über Zertifizierungen, Audits und technisch-organisatorische Maßnahmen zu kurz bemessen ist. Gerade vor dem Hintergrund, dass insbesondere bei den Unternehmen von besonderem öffentlichen Interesse ohnehin größerer Anpassungsbedarf ggfs. auch bei deren Zulieferbetrieben und Dienstleistern besteht und vor dem Hintergrund einer deutlichen Erweiterung des Adressatenkreises dieser Norm ist die vorgenommene Fristverkürzung vor allem in Verbindung mit dem gesetzten Bußgeldrahmen nicht nachvollziehbar. Die betroffenen Unternehmen benötigen angemessene Umsetzungs- und Implementierungsfristen.

Zu Artikel 1 Nr. 20

Der § 10 des BSI-Gesetzes sieht einen neuen Absatz 6 vor, der das BMI im Einvernehmen mit dem BMWi dazu ermächtigt, eine Verordnung über die „Offenlegung von Schnittstellen und die Einhaltung etablierter technischer Standards“ zu erlassen. In der vorliegenden Pauschalität ist die Verordnungsermächtigung abzulehnen. Die hier getroffene Regelung wird aller Voraussicht nach nicht mit den ohnehin bestehenden Maßgaben harmonieren. Inwieweit eine Offenlegung von Schnittstellen zur Verbesserung der IT-Sicherheit beitragen soll, wird nicht erläutert. Die Gesetzesbegründung lässt bedauerlicherweise keine weiteren Rückschlüsse zu, da sie gänzlich fehlt. Bisher war an anderer Stelle in Bezug auf die Offenlegung von Schnittstellen meist auf die Ausleitung von Kommunikation von Endnutzern bezogen. eco erachtet die hier getroffene Verordnungsermächtigung als verfassungsrechtlich problematisch, da hiervon unter Umständen auch ein grundrechtssensitiver Bereich tangiert

wird. Zudem sind Schnittstellen oftmals urheberrechtlich geschützt, was zusätzliche Probleme eröffnen dürfte. In der vorliegenden Fassung und Ausgestaltung ist diese Vorschrift abzulehnen.

Zu Artikel 2

Ergänzend zu den ausführlichen Ausführungen zum Diskussionsentwurf erachtet eco die in § 109 TKG-neu vorgeschlagenen Änderungen als Verletzung des Parlamentsvorbehalts. In der Allgemeinverfügung zum Sicherheitskatalog soll festgelegt werden können, was kritische Funktionen sind, anhand deren wiederum kritische Komponenten im Sinne von § 2 Abs. 13 BSIG-neu bestimmt werden und anhand dessen ein Betreiber öffentlicher Telekommunikationsnetze mit erhöhtem Gefährdungspotenzial einzustufen ist. Allein die beschriebene Herleitung und Verweisung macht deutlich, dass für betroffene Unternehmen keinerlei Vorhersehbarkeit besteht und selbst kleinere Änderungen und Anpassungen auf untergesetzlicher Ebene gravierende Auswirkungen und Konsequenzen für die Unternehmen haben können. Unter anderem sind mit den getroffenen Festlegungen eine Vielzahl intensiver Eingriffe bei den Unternehmen verbunden, wie beispielsweise die Meldepflicht einzelner Komponenten, der Untersagungsvorbehalt, eine Rückbauverpflichtung, die Durchführung von Audits im Zwei-Jahres-Intervall zusätzlich zu Überprüfungen durch BNetzA. Nach Ansicht des eco muss die Entscheidung und Festlegung der kritischen Komponenten sowie kritischen Funktionen innerhalb aller Sektoren auch im Bereich Telekommunikation zwingend durch den parlamentarischen Gesetzgeber getroffen und vorgenommen werden.

Fazit

Vor dem Hintergrund der vom BMI eingeräumten eintägigen Frist zur Beteiligung ist eine der Bedeutung des Gesetzgebungsverfahrens angemessene und umfangreiche Kommentierung nicht möglich. Insbesondere unter Berücksichtigung des Umstands, dass auch der nunmehr zur Verbändebeteiligung freigegebene Gesetzentwurf noch nicht endgültig ressortabgestimmt und weitere Änderungen zu erwarten sind, kann eine abschließende Bewertung des geplanten IT-SiG 2.0 im jetzigen Stadium nicht erfolgen. eco wird sich daher im weiteren Verlauf des Gesetzgebungsverfahrens zum IT-SiG 2.0 einbringen.

Die mit dem vorliegenden Referentenentwurf vorgenommen Anpassungen und neuen Regelungen verstärken die Bedenken, dass mit dem IT-SiG 2.0 in der derzeit diskutierten Form das Ziel einer stringenten, verhältnismäßigen und zielgerichteten IT-Sicherheitsregulierung für Deutschland mit einem klar umrissenen Anwendungsbereich nicht erreicht werden kann. Die bereits bestehenden grundsätzlichen Zweifel an Verfassungsmäßigkeit und

Verhältnismäßigkeit der geplanten Regelungen wurden mit dem nun vorgelegten Referentenentwurf weiter verstärkt und erfordern gravierenden Überarbeitungs- und Nachbesserungsbedarf.

eco – Verband der Internetwirtschaft e.V. empfiehlt in Anerkennung der Konsequenzen für den weiteren Gesetzgebungsvorgang, die Beratungen des IT-SiG 2.0 zurückzustellen und die weiteren Entwicklungen auf europäischer Ebene abzuwarten. Nur so kann eine systematische und stringente IT-Sicherheitsregulierung mit Erfolg umgesetzt werden.

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, schafft Rahmenbedingungen und vertritt die Interessen seiner Mitglieder gegenüber der Politik und in internationalen Gremien. Die Zuverlässigkeit und Stärkung der digitalen Infrastruktur, IT-Sicherheit und Vertrauen sowie eine ethisch orientierte Digitalisierung bilden Schwerpunkte der Verbandsarbeit. eco setzt sich für ein freies, technikneutrales und leistungsstarkes Internet ein.

[redacted]

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
19(4)748

Von: REPRAESENTANZ [mailto:repraesentanz@telefonica.com]
Gesendet: Donnerstag, 25. Februar 2021 11:45
Betreff: Telekommunikationsgesetz und IT-Sicherheit / Anhörung 1.3.

Sehr geehrte Damen und Herren Abgeordnete der Ausschüsse für Wirtschaft und Energie, Verkehr und digitale Infrastruktur, Inneres und Heimat, Digitale Agenda,

für die künftige Ausgestaltung des Rechtsrahmens der Telekommunikation in Deutschland beraten Sie derzeit über sehr wesentliche Gesetzgebungsverfahren. Der Entwurf der Novelle des Telekommunikationsgesetzes (BT 19/26108) und der Gesetzesentwurf zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2, BT 19/26106) sind die Basis für die Entwicklung der digitalen Infrastruktur in den kommenden Jahren. Aus Sicht von Telefónica / O2 wird von Ihren Entscheidungen abhängen, ob wir aus Fehlern der Vergangenheit lernen und stabile Rahmenbedingungen für die notwendigen immensen Investitionen in eine exzellente digitale Infrastruktur bekommen werden.

Beim Telekommunikationsgesetz (TKG) halten wir folgende Veränderungen im Gesetzgebungsprozess dringend für notwendig:

1.) Schaffung einer Frequenzpolitik, die investitionsfreundlich ist und daher keine Vorfestlegung auf ein einzelnes Vergabeverfahren (Auktion) vornimmt. Der Regierungsentwurf steht hier weder im Einklang mit dem umzusetzenden EU-Kodex noch lernt er aus den Fehlern der Vergangenheit, die zu einer im internationalen Vergleich spürbaren Investitionslücke geführt haben.
2.) Regelung von Übergangsfristen, um die komplexen Veränderungen umsetzen zu können. Das Fehlen jeglicher Übergangsfristen ist angesichts der notwendigen Anpassungen in sehr großen IT-Systemen mit etlichen Millionen Kunden nicht nachvollziehbar.

Beim IT-Sicherheitsgesetz gibt es trotz eines mittlerweile deutlich klareren Entwurfs nach wie vor nicht ausreichend geregelte Bereiche, die Betreiber von Telekommunikationsinfrastrukturen stark belasten:

1.) Die Verpflichtung zur Zertifizierung knüpft fälschlicherweise bei den Telekommunikationsbetreibern an. Es muss hier dringend eine klare Zuordnung von Verantwortlichkeiten erfolgen.
2.) Im Falle eines Ausschlusses eines Anbieters sind die Rechtsfolgen überhaupt nicht ausreichend geklärt. Es gibt keine Übergangsfristen, und es werden keine Schadensersatzregeln verankert. Es wäre sehr ratsam, diese Fragen im Gesetzgebungsverfahren und nicht erst gerichtlich einer Klärung zuzuführen.

Zu beiden Gesetzgebungsverfahren finden Sie unsere Stellungnahmen anbei. Wir bitten Sie dringend, die Entwürfe so zu verabschieden, dass die Rahmenbedingungen für Investitionen in exzellente digitale Infrastrukturen in Deutschland besser werden. Für weitere Informationen steht Ihnen das Government Relations-Team gerne zur Verfügung.

Mit den besten Grüßen

Philippe Gröschel, Harald Geywitz und Marina Grigorian

Telefónica Deutschland
Government Relations | Repräsentanz
Unter den Linden 26 10117 Berlin
T +49 (0)30 2369 1157
repraesentanz@telefonica.com | www.telefonica.de | www.basecamp.digital

Stellungnahme von Telefónica Deutschland zum Diskussionsentwurf eines zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-SiG 2.0)
Stand: 24. Februar 2021

Telefónica Deutschland (im weiteren Telefónica) ist mit 43,5 Millionen Mobilfunkanschlüssen und 2,2 Millionen Breitbandanschlüssen einer der führenden integrierten Telekommunikationsanbieter in Deutschland. Das Unternehmen bietet Mobilfunk- und Festnetzdienste für Privat- und Geschäftskunden an und betreibt eine eigene Mobilfunkinfrastruktur, die derzeit aus etwa 26.000 Mobilfunkstandorten sowie einem hochleistungsfähigen Verbindungs- und Kernnetz besteht. In den kommenden Jahren plant Telefónica, jährlich rund 1,3 Milliarden Euro in digitale Infrastruktur in Deutschland zu investieren.[1]

Telefónica begrüßt vor dem Hintergrund der aktuellen Bedeutung von Telekommunikationsnetzen für Wirtschaft und Gesellschaft in Deutschland eine steigende Sensibilität für Fragen der IT-Sicherheit.

Vor allem im Zuge der anstehenden Verabschiedung der NIS2 Richtlinie und der zwingenden Notwendigkeit eines stärker harmonisierten und zukunftsorientierten Cybersicherheitsrahmens auf europäischer Ebene weisen wir im Zusammenhang mit der nun diskutierten nationalen Regulierung jedoch ausdrücklich auf die Entwicklung und Umsetzung europaweit einheitlicher Standards hin. Vorgaben auf nationaler Ebene sollten zwingend mit den EU-Empfehlungen oder zukünftigen EU-Richtlinien harmonisiert werden.

Im vorliegenden Entwurf der Bundesregierung zum IT-Sicherheitsgesetz vom 16.12.2020 ist aus Sicht von Telefónica eine starke einseitige Belastung der betroffenen Mobilfunkunternehmen zu Grunde gelegt. Als Betreiberin einer kritischen Infrastruktur im Sinne des §2 Abs. 10 BSIG ist Telefónica unmittelbar von der geplanten Gesetzesänderung des IT-SiG 2.0 betroffen. Teile des vorliegenden Entwurfs der Bundesregierung haben Einfluss auf den Betrieb und Ausbau der digitalen Infrastruktur und die Geschäftstätigkeit von Telefónica.

In der vorliegenden Stellungnahme legt Telefónica einen Fokus auf ausgewählte Aspekte des Gesetzentwurfs und verweist im Übrigen auf die ausführlichen Stellungnahmen der Verbände Bitkom und VATM, zu deren Mitgliedern Telefónica zählt.

Im Speziellen legt Telefónica den Fokus dieser Kurzstellungnahme auf folgende Aspekte:

- **Massive rechtliche und ökonomische Risiken für die Betreiber von kritischen Infrastrukturen:** Sämtliche Folgen, die eine Untersagung der Nutzung einzelner Komponenten gemäß § 9b Abs. 3 BSIG-E hätte, sind im vorliegenden Gesetzentwurf nicht geregelt. Dringend erforderlich ist für das Szenario einer Untersagung eine Regelung, die eine mindestens fünfjährige Übergangsphase für den Rückbau und Austausch einzelner Komponenten vorsieht. Auch eine bisher gänzlich fehlende Regelung des Schadensersatzes sollte in das Gesetz aufgenommen werden. Es darf nicht sein, dass Betreiber, die in Deutschland private Mittel in den Ausbau kritischer Infrastrukturen investieren, den ökonomischen Schaden zu tragen haben, wenn der Bund aufgrund einer politischen Entscheidung Lieferanten dieser Betreiber als nicht vertrauenswürdig einstuft. Vor allem, wenn die infrage kommenden Komponenten zuvor durch eine Bundesbehörde geprüft und zertifiziert worden sind, der Betreiber der kritischen Infrastruktur also unverschuldet einen Schaden erleidet. Hier sollte im Falle einer potenziellen Untersagungsentscheidung dringend eine Kompensationsregelung gefunden werden, um einen stabilen Weiterbetrieb der Mobilfunknetze zu gewährleisten.
- **Keine Rechtssicherheit, da wesentliche Entscheidungen an Behörden ausgelagert werden:** Wesentliche Entscheidungen im Regime der Untersagung der Nutzung einzelner Komponenten würde der Gesetzgeber

[1] Weitere Fakten und Kennzahlen von Telefónica Deutschland finden Sie unter www.telefonica.de/unternehmen.html

mit dem vorliegenden Entwurf an die Verwaltung übertragen. Von den Anforderungen an die Garantieerklärung über die Liste kritischer Komponenten bis hin zum gesamten Ablauf und Inhalt des Zertifizierungsverfahrens sollen letztlich Behörden über Verordnungen, Verfügungen und Richtlinien das Sagen haben. Der vorliegende Gesetzentwurf bietet daher nicht die Rechtssicherheit, die für Betreiber kritischer Infrastrukturen dringend erforderlich wäre.

- **Bestandsnetze dürfen nicht von neuer Regulierung erfasst sein:** Es fehlen in dem Gesetzentwurf wichtige Überleitungsvorschriften, die festlegen, dass der Regulierungsmechanismus sowie die Folgen des § 9b BSIG-E nur für Komponenten angewendet werden, deren Nutzung zukünftig beim BMI angezeigt wird. Eine Rückwirkung auf Bestandsnetze muss schon aus Gründen des Investitions- und Vertrauensschutzes dringend ausgeschlossen werden.
- **Fehlende Rechtsfolgen:**

Im Einzelnen

1. Ausweitung der Aufgaben des BSI, § 3 BSIG-E

Der Gesetzentwurf intendiert die Einführung eines Parallelsystems, bei dem das BSI für den Bereich IT-Sicherheit mehrere zuvor voneinander getrennte Kompetenzen wie Standardisierung, Prüfung und Zertifizierung sowie typische Aufgaben von Sicherheits- und Strafverfolgungsbehörden gleichzeitig übernehmen soll. Ein derartiges Kompetenzgeflecht schafft unnötige zusätzliche Bürokratie, doppelte und längere Verfahren und verspielt das Potenzial für zügiges Verwaltungshandeln. Es steht zu befürchten, dass die Arbeit des BSI aufgrund des geplanten Wachstums der Behörde zur Innovationsbremse wird. Bürokratie und langsames Verwaltungshandeln würden letztlich zu weniger Rechtssicherheit und in letzter Konsequenz zu erheblichen Verzögerungen beim Ausbau von Netzen mit kritischen Komponenten führen. Telefónica plädiert aus diesen Erwägungen heraus dafür, dass die Aufgaben des BSI gesetzlich auf Schutzziele beschränkt werden.

2. Adressat der Zertifizierungspflicht, § 9 BSIG

Adressaten der Zertifizierungspflicht müssen die Hersteller kritischer Komponenten selbst sein. Dies sollte im IT-Sicherheitsgesetz klar festgelegt werden. Bisher ist im Gesetzesentwurf lediglich geregelt, dass kritische Komponenten von Betreibern nur eingesetzt werden dürfen, wenn eine Garantieerklärung der Hersteller über deren Vertrauenswürdigkeit vorliegt, die Komponente zertifiziert wurde und die Nutzung der Komponente beim BMI angezeigt wurde. Hier scheint der vorliegende Gesetzentwurf darauf zu vertrauen, dass die Betreiber von Infrastrukturen mit kritischen Komponenten die Frage, wer für die Zertifizierung einer Komponente überhaupt verantwortlich ist, auf vertraglicher Ebene mit den Herstellern klären. Da für die Durchführung der Zertifizierung jedoch zwingend die Mitwirkung sowie Dokumentationen und Fachkenntnisse des Herstellers erforderlich sind, sollte die Pflicht einer Zertifizierung klar an den Hersteller adressiert werden. Telefónica regt daher an, eine gesetzliche Regelung zu schaffen, die klarstellt, dass ein Hersteller, der kritische Komponenten in den Verkehr bringt, diese auch zertifizieren lassen muss. Adressat des Zertifizierungs-Regimes sollte nicht der Betreiber sein, sondern der Hersteller!

3. Voraussetzungen für Anmeldung kritischer Komponenten sind nicht hinreichend gesetzlich geregelt, § 9b Abs. 1, 2 BSIG-E

Zahlreiche Voraussetzungen und Definitionen, die für eine rechtssichere Anwendung des § 9b BSIG-E erforderlich sind, sollen später von Behörden auf untergesetzlicher Ebene definiert werden. Dies führt dazu, dass die potenziellen Folgen des § 9b BSIG-E basierend auf dem vorliegenden Entwurf nicht abschließend beurteilt werden können und die Wirksamkeit und Wirkungsweise des Mechanismus auch nach Abschluss des Gesetzgebungsverfahrens jederzeit von den Behörden geändert werden kann, indem einzelne Verordnungen geändert werden. Die Betreiber kritischer Infrastrukturen werden so auch nach

Inkrafttreten des IT-SiG 2.0 weiterhin keine Rechtssicherheit betreffend der Nutzung kritischer Komponenten zu erwarten haben.

Es ist derzeit unbekannt, welche Komponenten tatsächlich als kritische Komponenten im Sinne des Gesetzes anzusehen sind, da eine Liste der Komponenten gemäß § 2 Abs. 13 BSIG-E nachgelagert von BNetzA, BSI und BfDI festgelegt wird. Auch die Anforderungen an die Garantieerklärung sollen nach § 9b Abs. 2 BSIG-E erst zu einem späteren Zeitpunkt im Zuge der Allgemeinverfügung durch das BSI festgelegt werden. Schließlich werden auch Ablauf und Inhalt des zwingend zu durchlaufenden Zertifizierungsverfahrens durch das BSI festgelegt, ohne dass diese schon jetzt bekannt wären, siehe § 9 Abs. 4 BSIG-E. Da all diese Voraussetzungen für die Anmeldung der Nutzung kritischer Komponenten beim BSI im Sinne des § 9b Abs. 1 BSIG-E jedoch zwingend bekannt sein müssen, ist das aktuell vorgesehene Regime der Untersagung stark von Entscheidungen der Behörden und faktischem Verwaltungshandeln abhängig.

Während bei der Erstellung der Liste kritischer Komponenten sowie bei der Ausgestaltung des Zertifizierungsverfahrens für eine Ermächtigung der Behörden sprechen könnte, dass auf diese Weise ein innovationsoffener und technologieneutraler Ansatz in der Gesetzgebung gewählt wird, ist es nicht ersichtlich, warum Anforderungen an die Garantieerklärung nicht von vornherein gesetzlich geregelt werden können. Aus Sicht von Telefónica sollte der Gesetzgeber sich daher nicht davor drücken, über entscheidende Definitionen und Voraussetzungen selbst zu entscheiden.

4. Fehlende Regelung zu den Folgen im Falle einer Untersagung führen zu unverhältnismäßiger Belastung der Betreiber, § 9b Abs. 3, 4 BSIG-E

a. Pflichten des § 9b belasten einseitig die Betreiber

Die Auferlegung sämtlicher Pflichten und Risiken des § 9b BSIG-E auf die Schultern des Betreibers - von der Einholung der Garantieerklärung für kritische Komponenten und deren Administration über die potenziellen betrieblichen und wirtschaftlichen Folgeschäden durch die Einbeziehung von Behörden bis hin zur Untersagung eines Komponenteneinsatzes - ist unverhältnismäßig. Das Vorgehen greift durch die Zwangsvorgaben auch in das EU-Ausschreibungsrecht zu Lasten der betroffenen Unternehmen ein und führt ggf. zu Marktverzerrungen wegen Ungleichbehandlung.

b. Übergangsregelung für den Phase-Out

Für den Fall, dass es aufgrund mangelnder Vertrauenswürdigkeit ultima-ratio zu einer Untersagung der Nutzung einer kritischen Komponente kommt, ist dringend eine Übergangsregelung von mindestens fünf Jahren erforderlich, die einen Rückbau bzw. Austausch der Komponenten ermöglicht, ohne dass der Betrieb und der weitere Ausbau der Infrastruktur dadurch massiv beeinträchtig werden. Neben den angemessenen Übergangsfristen für einen eventuellen Rückbau bereits verbauter Komponenten muss eine Norm für die Risikoübernahme bzw. entsprechende Entschädigungen für die Aufwendungen vorgesehen werden.

c. Kompensationsregelung

Nach der derzeitigen Regelung kann es im Falle einer potenziellen Untersagung zur unverhältnismäßigen Belastung von Betreibern der kritischen Infrastrukturen kommen. Die potenziellen wirtschaftlichen sowie betrieblichen Folgeschäden dürfen auf keinen Fall zu Lasten der Betreiber gehen. Sollte es trotz einer Zertifizierung der Komponenten und einer wirksam erteilten Garantieerklärung dennoch aufgrund einer später festgestellten fehlenden Vertrauenswürdigkeit zu einer politisch beschlossenen Untersagung kommen, sollte eine spezialgesetzliche Regelung die verschuldensabhängige Herstellerhaftung festlegen. Eine solche Regelung allein kann die wirtschaftlichen Risiken der Betreiber jedoch nicht ausreichend kompensieren. Wenn ein Hersteller tatsächlich aufgrund fehlender Vertrauenswürdigkeit de facto vom deutschen Markt ausgeschlossen werden würde, so würde er sich vermutlich binnen kurzer Zeit sehr hohen Schadensersatzforderungen ausgesetzt sehen. Das Risiko der Insolvenz des Herstellers wäre in diesem Fall unkalkulierbar groß, was wiederum zu einem nicht tragbaren Risiko für die Betreiber werden würden. Aus diesem Grund sollte als zweite Stufe, wenn

Schadensersatzansprüche der Betreiber nicht aus einer Herstellerhaftung befriedigt werden können, auch eine Haftung des Staates für die Folgen des Ausschlusses geregelt werden. Nach Ansicht von Telefónica sollte dieser Aspekt dringend unmittelbar im BSIG geregelt werden. Daher wird vorgeschlagen, einen neuen §14b in das Gesetz aufzunehmen, der folgend lauten könnte:

> *§14b Zur Entschädigung verpflichtende Maßnahmen*
>
> *(1) Ein Hersteller, der sich nach § 9b Abs. 4, Abs. 5 als nicht vertrauenswürdig erwiesen hat, ist dem Betreiber zum Ersatz des daraus entstandenen Schadens verpflichtet. Satz 1 kann nicht vertraglich ausgeschlossen werden.*
>
> *(2) Erhält der Betreiber keinen Ersatz für den Schaden nach Abs. 1 oder auf andere Weise, so ist ihm der Schaden zu ersetzen, der infolge einer Inanspruchnahme nach § 9b Abs. 4 entstanden ist, gleichgültig, ob das BMI ein Verschulden trifft oder nicht.*
>
> *(3) Soweit die Entschädigungspflicht wegen rechtmäßiger Maßnahmen der Ordnungsbehörden in anderen gesetzlichen Vorschriften geregelt ist, finden diese Anwendung.*
>
> *(4) Die Entschädigung nach Abs. 2 wird für entgangenen Gewinn und alle Vermögensschäden gewährt, unabhängig davon, ob sie in einem unmittelbaren Zusammenhang mit der zu entschädigenden Maßnahme stehen oder nicht.*
>
> *(5) Hat bei der Entstehung des Schadens ein Verschulden des Betreibers mitgewirkt, so ist das Mitverschulden bei der Bemessung der Entschädigung zu berücksichtigen.*
>
> *(6) Soweit die zur Entschädigung verpflichtende Maßnahme auch eine Amtspflichtverletzung darstellt, bleiben die weitergehenden Ersatzansprüche unberührt.*
>
> *(7) Für die Verjährung des Entschädigungsanspruchs gelten die Bestimmungen des Bürgerlichen Gesetzbuchs über die Verjährung von Schadensersatzansprüchen entsprechend.*
>
> *(8) Entschädigungspflichtig ist die Bundesrepublik Deutschland.*
>
> *(9) Über die Entschädigungsansprüche nach dieser Vorschrift entscheiden im Streitfall die ordentlichen Gerichte.*

Anderenfalls sind die Betreiber, die aus privaten Mitteln die Digitalisierung und die Positionierung Deutschlands als 5G-Leitmarkt vorantreiben, unverhältnismäßig und einseitig belastet.

Analog der Regelung zur Entschädigung der Energiewirtschaft bei der Energiewende sollte für betroffene Mobilfunkunternehmen ein **Netzbetriebs-Stabilitätsfonds** eingerichtet werden, um eine reibungslose, stabile Weiterversorgung sowie den flächendeckenden Ausbau der Mobilfunknetze der nächsten Generation zu gewährleisten. Dies wäre insbesondere dann dringend erforderlich, wenn die von den Folgen der Untersagung negativ betroffenen Betreiber kritischer Infrastrukturen rechtlich und tatsächlich keine Möglichkeit haben, ihren Schaden durch Ansprüche gegenüber den Lieferanten der entsprechenden Komponenten zu kompensieren, beispielsweise weil Lieferanten in Deutschland in Folge des Marktausschlusses insolvent sind.

5. Technische Zertifizierung kritischer Komponenten, § 2 Abs. 13 BSIG-E, § 109 Abs. 2 TKG-E

Grundsätzlich bewertet Telefónica den Ansatz positiv, dass kritische Komponenten einer Zertifizierung unterzogen werden sollen und ist bereit, sich im Dialog mit dem BSI in die Entwicklung und regelmäßige Evaluation des Zertifizierungsverfahrens einzubringen.

Kritische Komponenten bzw. Komponenten mit kritischen Funktionen können i. S. dieses Gesetzes nur dann kritisch sein, wenn ihre Funktionalitäten in Bezug auf die Einsatzumgebung im Falle ihrer Beeinträchtigung den KRITIS-Schutzzielen zuwiderlaufen. Daher sollte die Zertifizierung sich nur auf ausgewählte Elemente des Kernnetzes konzentrieren, da hier die Datenströme aus dem Zugangsnetz zusammenlaufen sowie zentrale Netzfunktionalitäten und Datenbanken angesiedelt sind, wodurch diese primär zum Ziel eines Angriffs werden

könnten. Eine Einbeziehung der Zugangsnetze dürfte Zertifizierungsverfahren und Vertrauenswürdigkeitsprüfung zu einem Bottleneck machen. Die in § 2 Abs. 13 BSIG-E zugrunde gelegte Definition kritischer Komponenten sollte nach Auffassung von Telefónica daher dringend auf solche Komponenten beschränkt werden, die in zentralen Netzwerkebenen zum Einsatz kommen.

Ebenfalls wichtig ist, dass Zertifizierungen anderer EU-Behörden ohne weitere Hürden anerkannt werden. Wenn eine Komponente von einer Behörde eines anderen EU-Mitgliedsstaates zertifiziert wurde, sollte diese nicht erneut beim BSI vorgelegt werden müssen.

6. Keine rückwirkende Belastung für Bestandsnetze, § 9b Abs. 4 BSIG-E

Eine Untersagung des Einsatzes von bereits eingesetzten Komponenten zum Zeitpunkt des Inkrafttretens des Gesetzes muss ausgeschlossen werden (Bestandsschutz). Im Sinne eines Investitionsschutzes dürfen die Folgen einer möglicherweise festgestellten mangelnden Vertrauenswürdigkeit sich nicht auf Komponenten erstrecken, die bereits vor Inkrafttreten des IT-SiG 2.0 verbaut wurden. Es bedarf zudem einer Klarstellung, dass auch die Pflicht zur Meldung des Einsatzes kritischer Komponenten an das BMI sich nicht auf bereits im Netz verbaute Komponenten beziehen darf (die z. B. im Rahmen einer Wartung oder Fehlerbehebung ausgetauscht werden müssen), sondern nur auf solche Komponenten, die erstmals neu im Netz in Betrieb genommen werden. Im Gesetz bedarf es daher dringend einer entsprechenden Überleitungsvorschrift, die klarstellt, dass das gesamte Regelungsregime des § 9b BSIG-E nur für Komponenten einschlägig ist, die zukünftig neu im Netz verbaut werden.

7. Ermächtigung zum Erlass von Rechtsverordnungen, § 10 Abs. 6 BSIG-E

Telefónica begrüßt den hier angestrebten Ansatz, IT-Security als einen dynamischen Prozess und nicht als ein starres Konstrukt zu begreifen. Das gesuchte Einvernehmen mit dem Bundesministerium für Wirtschaft und Energie sowie die Einbeziehung der Wirtschaftsverbände begrüßen wir ebenfalls.

Dennoch sehen wir es als äußerst kritisch an, dass die Interoperabilität und Schnittstellenkompatibilität von Komponenten und Systemen pauschal und unabhängig von deren Kritikalität und/oder Funktionalität über eine Verordnung geregelt werden kann. Dies konterkariert die Bestrebungen des vorliegenden Gesetzentwurfs, der im Wesentlichen auf kritische Komponenten bzw. kritische Funktionen abstellt. Zudem steht es im krassen Widerspruch zu einer EU-weiten Harmonisierung der IT-Sicherheitsregulierung, dass hier die nationalen Behörden unabhängig von EU-Standards selbst Vorgaben zu technischen Standards machen können. Diese sehr weit und unbestimmt gefasste Vorschrift muss im Sinne des Bestimmtheitsgrundsatzes, sowie um Rechts- und Planungssicherheit für die betroffenen Unternehmen zu ermöglichen, zwingend angepasst und konkretisiert werden. Denkbar wäre hier eine Eingrenzung auf die Liste der kritischen Funktionen und Komponenten nach § 109 Abs. 6 TKG-E und die Einbeziehung der Maßnahmen nach der EU-5G-Tool-Box.

Ansprechpartner

Philippe Gröschel, Head of Government Relations, philippe.groeschel@telefonica.com

Stellungnahme von Telefónica Deutschland zum Kabinettsentwurf des Gesetzes zur Modernisierung des Telekommunikationsrechts (TKG-E) vom 16. Dezember 2020

Stand der Stellungnahme: Februar 2021

Telefónica Deutschland (im weiteren Telefónica) ist mit 44,3 Millionen Mobilfunkanschlüssen und 2,3 Millionen Breitbandanschlüssen einer der führenden integrierten Telekommunikationsanbieter in Deutschland. Das Unternehmen bietet Mobilfunk- und Festnetzdienste für Privat- und Geschäftskunden an und betreibt eine eigene Mobilfunkinfrastruktur, die derzeit aus etwa 26.000 Mobilfunkstandorten sowie einem hochleistungsfähigen Verbindungs- und Kernnetz besteht. In den kommenden Jahren plant Telefónica jährlich rund 1,3 Milliarden Euro in digitale Infrastruktur in Deutschland zu investieren.[1]

Weite Teile des vorliegenden Regierungsentwurfs zur Modernisierung des Telekommunikationsgesetzes vom 16.12.2021 (im weiteren TKG-E) haben unmittelbaren Einfluss auf die Geschäftstätigkeit und die Produkte von Telefónica. Weil es sich bei dem TKG-E um das vermutlich wichtigste Gesetzgebungsverfahren im Bereich der Telekommunikationsregulierung in den nächsten Jahren handelt, sieht Telefónica es kritisch, dass bei zahlreichen Abschnitten des Gesetzes noch Klärungsbedarf in technischer und rechtlicher Hinsicht besteht. Dies ist auch damit begründet, dass die Konsultationsfrist der Entwürfe im Vorfeld des Kabinettsbeschlusses vom 16.12.2020 deutlich zu kurz war und damit die Chance verpasst wurde, mit den betroffenen Kreisen ungenaue Formulierungen klarzustellen und besser umsetzbare Lösungen zu erarbeiten.

Aus Sicht von Telefónica sollte sich der Gesetzgeber in Deutschland bei der Überarbeitung des Telekommunikationsrechts noch stärker darauf fokussieren, das überragende politische Ziel, die privaten Investitionen in digitale Infrastruktur in Deutschland zu erhöhen und damit den Netzausbau zu beschleunigen, zu fördern. An vielen Stellen erhöht der Gesetzentwurf das ohnehin schon intensive Regulierungsniveau für den Telekommunikationssektor und führt neue, in ihrer Umsetzung aufwendige Pflichten ein, ohne ausreichenden Ausgleich auf der Seite der Investitionsanreize zu bieten. An den vielen Stellen, wo das Regulierungsniveau des bisher vorliegenden Gesetzesentwurfs über den EECC hinausgeht, sollte der Gesetzgeber hinterfragen, ob eine zusätzliche Belastung der Telekommunikationsunternehmen in Deutschland erforderlich und angemessen ist.

In der vorliegenden Stellungnahme legt Telefónica einen Fokus auf ausgewählte Aspekte des Gesetzentwurfs und verweist im Übrigen auf die ausführlichen Stellungnahmen der Verbände Bitkom und VATM, zu deren Mitgliedern Telefónica zählt.

Im speziellen regt Telefónica Änderungen in folgenden Bereichen des Gesetzentwurfs an:

- Im Bereich der Regulierung des **Kundenschutzes** umfasst der Entwurf des TKG-E zahlreiche Regelungen, die über den EECC hinausgehen und damit eine Schlechterstellung von in Deutschland tätigen Telekommunikationsunternehmen im Vergleich zu europäischen Wettbewerbern darstellen. Konkret sollten die Regelungen zur Bereitstellung der Vertragszusammenfassung, zum

[1] Weitere Fakten und Kennzahlen von Telefónica Deutschland finden Sie unter www.telefonica.de/unternehmen.html

Minderungsrecht bei Parameterabweichungen, zu Gebühren bei der Portierung von Rufnummern sowie zur Sperre bei Zahlungsverzug aus Sicht von Telefónica überarbeitet werden.

- Wir begrüßen, dass nach dem derzeitigen TKG-E weiterhin Verträge mit einer anfänglichen **Vertragslaufzeit** von 24 Monaten angeboten werden dürfen. Ausdrücklich wenden wir uns aber gegen eine Preisregulierung der zusätzlich zwangsweise anzubietenden 12-Monatsverträge. Diese Regelung greift tief in die Vertragsfreiheit der Telekommunikationsunternehmen ein und verteuert die Vermarktung durch einen erheblichen, neuen Bürokratieaufwand. Auch die Rechtsfolge der Unwirksamkeit eines längeren Laufzeitvertrages für den Fall, dass eine kürzere Laufzeit zuvor nicht angeboten wurde, ist unverhältnismäßig, führt zu neuem Dokumentationsaufwand und eröffnet rechtliche Risiken für Verbraucher und Unternehmer.
- Der in Deutschland gültige Rahmen der **Frequenzregulierung** wurde im Kontext der 2019 stattgefundenen Versteigerung von Frequenznutzungsrechten für 5G intensiv diskutiert. Dies führte allerdings bisher nicht zu einer Modernisierung der veralteten Systematik der Frequenzbereitstellung. Die im Gesetzentwurf weiterhin bestehende Vorprägung zu Gunsten des Versteigerungsverfahrens im Falle einer Frequenzknappheit ist kontraproduktiv und schließt alternative Vergabemodelle faktisch von vornherein aus. Die neu eingeführte Regelung zur Verlängerung von Frequenznutzungsrechten ist in ihrer Systematik nahezu unverständlich und würde in ihrer bisherigen Ausgestaltung voraussichtlich nicht greifen.
- Die im Gesetzentwurf der Bundesregierung geschaffene Angebotspflicht von Telekommunikationsunternehmen gegenüber dem **Behördenfunk BOS** lehnt Telefónica entschieden als Eingriff in die Privatautonomie der Netzbetreiber ab. Es darf nicht sein, dass der Staat sich selbst in seiner Rolle als Gesetzgeber eine Angebots- und Verhandlungspflicht zu seinen Gunsten schafft, anstatt auf und freiwilliger kommerzieller Basis als Nachfrager mit den Netzbetreibern über einen solchen Zugang zu verhandeln.
- Dringend sollten im TKG-E angemessene **Umsetzungsfristen** definiert werden, die eine technische und organisatorische Implementierung der neuen Regelungen möglich machen. Viele Anforderungen des TKG-E erfordern Anpassungen in bestehender Software sowie die Schulung des Personals im Bereich der Kundenbetreuung. Dies ist nur innerhalb einer Umsetzungsfrist von mindestens 12 Monaten zu realisieren.
- Neben den Umsetzungsfristen fehlen im Entwurf der Bundesregierung auch **Überleitungsvorschriften**, die eine **Rückwirkung** neuer Vorschriften auf bestehende Vertragsverhältnisse Regeln. Um Klarheit und Zuverlässigkeit im Rechtsverkehr zu erhalten, sollte der Gesetzgeber aus Sicht von Telefónica dringend klarstellen, dass eine Rückwirkung auf bereits bestehende Rechtsverhältnisse ausgeschlossen ist und neue gesetzliche Vorschriften nur für Rechtsverhältnisse nach Inkraft-Treten des TKE-E Anwendung finden.

Im Einzelnen

1. Kundenschutz

a. Vertragszusammenfassung und Folgen verspäteter Bereitstellung (§ 54 Abs. 3 TKG-E)

Die Vorgaben zum Zeitpunkt und zur Form der Bereitstellung der Vertragszusammenfassung und die Regelungen bei deren verspäteter Bereitstellung gehen weit über die Vorgaben des EECC hinaus und verletzen das Prinzip der Vollharmonisierung nach Art. 101 Abs. 1 EECC:

aa. Die in der Begründung des TKG-E enthaltene Formvorgabe geht weit über die Vorgaben des EECC hinaus, findet keinen Anknüpfungspunkt im Normtext des § 54 Abs. 3 TKG-E und widerspricht sogar den Vorgaben des EECC. Während die vorvertraglichen Informationen auf einem dauerhaften Datenträger oder in einem leicht herunterladbaren Dokument bereitgestellt werden müssen (Art. 102 Abs. 1 EU-Kodex), sieht der EU-Kodex für die Vertragszusammenfassung gerade keine bestimmte Form vor (vgl. Art. 102 Abs. 3 EU-Kodex). Dennoch wird in der Gesetzesbegründung des TKG-E nun davon ausgegangen, dass die Vertragszusammenfassung stets auf einem dauerhaften Datenträger zur Verfügung gestellt werden muss. Dieses Verständnis würde dazu führen, dass der fernmündliche Vertragsschluss faktisch unmöglich gemacht würde. Dies hat der EU-Gesetzgeber gerade nicht intendiert, weshalb die Erteilung der Vertragszusammenfassung an keine bestimmte Form gebunden ist. Eine derart wesentliche Abweichung vom Normwortlaut des EU-Kodex verletzt das Prinzip der Vollharmonisierung nach Art. 101 Abs. 1 EECC. Telefónica regt daher eine gesetzliche Klarstellung in § 54 Abs. 3 TKG-E.

bb. Nach dem TKG-E soll die Vertragszusammenfassung dem Kunden bereits vor Abgabe seiner Vertragserklärung zugehen. Der EECC sieht jedoch vor, dass die Vertragszusammenfassung gegenüber dem Kunden lediglich “vor Vertragsschluss”, also nach Abgabe der Bestellung des Kunden, aber vor deren Annahme durch den Anbieter erfolgen muss. Der TKG-E verlagert die Pflicht der Bereitstellung der Zusammenfassung damit zeitlich nach vorne. Dies widerspricht den eindeutigen Vorgaben des Kodex, verletzt das Prinzip der Vollharmonisierung und hat erhebliche negative Auswirkungen auf den Vertriebsprozess. Im Übrigen würde die Zusendung einer *Vertrags*zusammenfassung vor Abgabe seiner Vertragserklärung beim Verbraucher naheliegender Weise den Verdacht erwecken, ihm werde ein *Vertrag* untergeschoben, obwohl er noch gar keine auf den Vertragsschluss gerichtete Willenserklärung abgegeben hat. Dies führt zu einer Verunsicherung des Verbrauchers. Telefónica regt deshalb an, § 54 Abs. 3 Satz 1 TKG-E entsprechend den Vorgaben den Kodex dahin zu ändern, dass die Vertragszusammenfassung „vor Abschluss des Vertrages“ bereitgestellt werden muss, jedoch nach der Erklärung der auf den Vertragsschluss gerichteten Willenserklärung des Verbrauchers erfolgen kann.

cc. Zu streichen sind die Regelungen der §§ 1-3 der in Art. 42 TKModG angepassten TK-Transparenzverordnung. Diese Regelungen sehen u.a. eine Bereitstellung der Vertragszusammenfassung bereits ab Beginn der Vermarktung des jeweiligen Tarifs vor, entsprechend der jetzigen Regelung für die Produktinformationsblätter. Diese Regelungen sind redundant zum System der Bereitstellung nach § 54 Abs. 3 TKG-E und stellen die inhaltliche Gestaltung der Vertragszusammenfassungen in Frage. Nach der Durchführungsverordnung (EU) 2019/2243 der Kommission sind in der Vertragszusammenfassung unter anderem Rabatte, Gerätepreise oder Sonderangebotspreise auszuweisen, so dass Vertragszusammenfassungen letztlich spezifisch bestellbezogene Preiskomponenten enthalten sollen. Bei einer Bereitstellung von Vertragszusammenfassungen bereits zu Beginn der Vermarktung wäre es nicht möglich, spezifisch bestellbezogene Preisinformationen anzugeben. Zu diesem Zeitpunkt könnten lediglich die Standardkonditionen des Tarifs ausgewiesen werden, so wie derzeit in den Produktinformationsblättern.

dd. Das Erfordernis einer Genehmigung in Textform bei verspäteter Bereitstellung der Vertragszusammenfassung geht ebenfalls über die Vorgaben des EECC hinaus, der in Artikel 102 Abs. 3 eine formfreie Bestätigung des Einverständnisses vorsieht. Für die Bestätigung in Textform kann auch nicht – wie in der Begründung zum TKG-E – die besondere Bedeutung dieser Erklärung herangezogen werden. Es wäre widersprüchlich, dass die Vertragserklärung selbst formfrei ist, die Genehmigung des Vertrages aber nicht. Auch andere gestaltende Erklärungen, wie z.B. der Widerruf des Verbrauchers beim Fernabsatzgeschäft, sind formfrei möglich. Telefónica regt deshalb an, in § 54 Abs. 3 Satz 4 TKG-E die Worte *„in Textform"* zu streichen.

ee. Letztlich ist auch die Regelung in § 54 Abs. 3 Satz 5 TKG-E, die eine Berechnung der vertraglichen Entgelte oder von Wertersatz nur im Falle der Genehmigung durch den Verbraucher zulässt, nicht vom EU-Kodex vorgesehen. Es ist nicht ersichtlich, weshalb der Verbraucher im Hinblick auf eine bestellte und ggf. auch bewusst in Anspruch genommene Leistung nicht entgeltpflichtig werden sollte. Dies kann zudem Missbrauch begünstigen, zumal die Vorschrift nach § 66 Abs. 1 TKG-E auch für Angebotspakete und somit u.U. auch für bereitgestellte Endgeräte gilt. Durch den zusätzlichen Ausschluss des Wertersatzes wird zudem das Bereicherungsrecht außer Kraft gesetzt, was ebenfalls mit dem Vollharmonisierungsansatz nicht zu vereinbaren ist. Schließlich ergibt sich auch ein Widerspruch zu § 357 Abs. 8 BGB, (sowie im Fall von Angebotspaketen ggf. zusätzlich zu § 357 Abs. 7 BGB) der abweichende Regelungen zum Wertersatz bei Verträgen regelt, bei denen ein Widerrufsrecht besteht. Telefónica regt an, § 54 Abs. 3 S. 5 TKG-E ersatzlos aus dem Gesetzentwurf zu streichen

b. Bereitstellung der Vorvertraglichen Informationen (§ 54 Abs. 1 TKG-E)

Aus Sicht von Telefónica sollte es stets ausreichen, dem Kunden die vorvertraglichen Informationen im Rahmen des Bestellprozesses auf einem leicht herunterladbaren Dokument zur Verfügung zu stellen. Gemäß § 54 Abs. 2 TKG-E soll dies jedoch nur ausreichend sein, wenn eine Bereitstellung auf einem dauerhaften Datenträger „nicht möglich" ist. Nach dem verbindlichen, englischen Richtlinienwortlaut soll eine herunterladbare Information dagegen bereits dann genügen, wenn die Bereitstellung auf einem dauerhaften Datenträger „nicht praktikabel" („not feasible") ist. Telefónica regt an, § 54 Abs. 1 TKG-E entsprechend anzupassen.

c. Anfängliche Vertragslaufzeit (§ 56 Abs. 1 TKG-E)

Wir begrüßen, dass sich eine Verkürzung der anfänglichen Vertragslaufzeit auf 12 Monate, wie sie bisher immer wieder diskutiert wurde aktuell nicht im Entwurf des neuen TKG findet. Eine solche Regelung ist weder erforderlich noch angemessen. Bereits heute sind alle Telekommunikationsanbieter im Mobilfunk und Festnetz dazu verpflichtet, auch einen Tarif mit einer 12-monatigen Laufzeit anzubieten. Eine generelle Verpflichtung, nur 12-monatige Verträge anbieten zu dürfen, würde für den Verbraucher keine Verbesserung bedeuten. Es existieren auch aufgrund von Nachfrage und Wettbewerb zahlreiche Tarife und Angebote mit kürzeren Vertragslaufzeiten. Jeder Verbraucher hat die freie Wahl, ob er sich - unter Abwägung der jeweiligen Vor- und Nachteile - 24, 12 oder noch weniger Monate binden oder aber einen Prepaid-Tarif wählen möchte. Tatsächlich entscheiden sich viele Verbraucher für Laufzeitverträge mit einer 24-monatigen Bindung, da sie die Sicherheit, Kontinuität und Preisstabilität einer verlässlichen Versorgung schätzen. Viele Verbraucher profitieren zudem von den Vorteilen der Kombi-Verträge und der Möglichkeit, Endgeräte kostengünstig bei gleichzeitigem Abschluss eines 24-Monats-Vertrages zu erhalten. Ähnliches gilt für

Festnetz- und DSL-Anschlüsse. Die hohen Erst-Anschlusskosten (Technikereinsatz bei Leitungsschaltung) werden hier sukzessive über die Laufzeit von 24 Monaten kompensiert. Ein pauschales Verbot von 24-monatigen Vertragslaufzeiten würde die Vorteile von Laufzeitverträgen deutlich verringern, zu steigenden Preisen führen und die Angebotsvielfalt zu Lasten der Verbraucher einschränken.
Eine generelle Verkürzung der maximalen Vertragslaufzeiten würde es für die Telekommunikationsanbieter erheblich erschweren, den zukünftigen Umsatz zu prognostizieren und damit die Investitionsmöglichkeiten begrenzen. Dies würde beispielsweise den investitionsintensiven, möglichst flächendeckenden Ausbau von hochleistungsfähigen Mobilfunknetzen konterkarieren und die Investitions- und Planungssicherheit derjenigen Unternehmen verschlechtern, die in die digitale Infrastruktur und Zukunft investieren.
Ausdrücklich wenden wir uns aber gegen die in § 56 Abs. 1 S. 2 TKG-E vorgesehene Preisregulierung der zusätzlich zwangsweise anzubietenden 12-Monatsverträge. Dies stellt einen erheblichen Eingriff in die Vertragsfreiheit dar. Vor Abschluss eines jeden Zweijahresvertrages und damit zu hunderten von Produktvarianten sollen den Kunden in Zukunft zwangsweise Verträge mit einjähriger Laufzeit zu regulierten Konditionen angeboten werden. Diese im deutschen Recht einmalige Regelung würde die Entwicklung und Vermarktung neuer Tarife durch einen erheblichen, neuen Bürokratieaufwand verkomplizieren. Zudem ist die vorgeschlagene Regelung unnötig, da bereits heute Verträge mit einjähriger oder sogar noch kürzerer Laufzeit angeboten werden müssen und weiterhin Monats- und Prepaid-Verträge im Markt verfügbar sind.

Darüber hinaus ist auch eine angemessene Überleitungsvorschrift für diese Regelung zu ergänzen. Während das Gesetz für faire Verbraucherverträge („FVVG“) in Art. 2 eine klare Überleitungsvorschrift zur Vermeidung von unerwünschter Rückwirkung enthält, fehlt eine solche Regelung im TKG-E trotz z.T. identischer Neuregelungen. Wir können keine Gründe erkennen, die eine Abweichung allein zu Lasten des TK-Sektors rechtfertigt. Denn gerade im TK-Sektor führen fehlende Überleitungsvorschriften vielfach auch in den Bereich verfassungsrechtlich problematischer Rückwirkung.

d. Tarifberatung in Textform (§ 57 Abs. 3 TKG-E)

Nach der Begründung zu § 57 Abs. 3 TKG-E soll die jährliche Tarifberatung auf einem dauerhaften Datenträger erfolgen. Dies missachtet, dass der Kodex gerade keine Formvorgaben zur Tarifberatung macht. Damit missachtet der TKG-E auch hier das Prinzip der Vollharmonisierung. Die Vorgabe kann zu erheblichen Mehraufwänden, Mehrkosten und Ressourcenverbrauch führen, wenn Kunden z.B. keine E-Mail-Adresse angeben möchten und eine Information dann per Post erfolgen müsste.

Zudem ist nicht nachvollziehbar, weshalb eine Tarifberatung auch dann nach einem Jahr erfolgen soll, wenn die anfängliche Mindestvertragslaufzeit 24 Monate beträgt. Telefónica regt an, dass Erfordernis, die Tarifberatung auf einem dauerhaften Datenträger zu erfolgen hat, aus der Begründung zu § 57 Abs. 3 TKG-E zu streichen und klarzustellen, dass eine Beratung jährlich, frühestens aber zum Ablauf einer vereinbarten Mindestlaufzeit erfolgen soll.

e. Minderungsrecht bei Abweichung von Geschwindigkeit oder anderen Diensteparametern (§ 57 Abs. 4 TKG-E)

Das im Regierungsentwurf geregelte Minderungsrecht bei Abweichung von Geschwindigkeit und anderen Qualitätsparametern ist aus der Sicht von Telefónica ein erheblicher und nicht gerechtfertigter Eingriff in die Geschäftstätigkeit. Zwei Beispiele zeigen, warum das Minderungsrecht etablierte Geschäftsmodelle im Telekommunikationsmarkt erheblich beeinträchtigt. Bei einem Mobilfunkanschluss variiert die Bandbreite je nach Standort und lokaler Nutzung des Mobilfunknetzes durch den Kunden. Für den Mobilfunkbereich ist daher eine solche Regelung problematisch, da der Kunde die Bandbreitenmessungen z. B. in einem Keller vornehmen kann, in dem kein oder nur sehr eingeschränkter Empfang besteht. In diesem Fall würde er die Leistung um 100 % mindern können, auch wenn die Leistung ansonsten einwandfrei nutzbar ist. Auch unterscheidet sich die Bandbreite je nach Standort. So kann die Messung vom Kunden dadurch beeinflusst werden, wo die Messung vorgenommen wird. Dadurch könnte der Kunde die Kosten seines Mobilfunkvertrages selbst beeinflussen.

Auch Produkte, die auf Festnetzvorleistungen basieren, werden durch das Minderungsrecht gefährdet. In der Regel können Marktteilnehmer als Vorleistung nur einen bestimmten Bandbreitenbereich bestellen, ohne die tatsächliche Bandbreite vorab ermitteln zu können. Wenn die Bandbreite vom Vorleistungserbringer nicht ausreichend erbracht wird, hätte der Kunde ein Minderungsrecht gegenüber seinem Anbieter. Dabei kann es zu der Situation kommen, dass der Kunde weniger Entgelt zahlen muss als der Anbieter selbst für die Vorleistung. Diese Minderung kann nach den derzeitig regulierten Verträgen der Telekom („Bitstream Access“) auch nicht an den Vorleistungserbringer “weitergegeben” werden, da sich das Leistungsversprechen der Telekom auf eine Übertragungsgeschwindigkeit innerhalb eines relativ breiten Korridors beschränkt. So liegt beispielsweise die Download-Geschwindigkeit für einen Vorleistungsanschluss mit einer Bandbreite von 100 Mbit/s gemäß den Vorleistungsverträgen der Telekom innerhalb eines Korridors von 55 Mbit/s (minimal erwartete Geschwindigkeit) bis 100 Mbit/s (maximale Geschwindigkeit). Zudem ist die Erreichbarkeit der in der Produktspezifikation angegebenen Übertragungsgeschwindigkeit generell unter den Vorbehalt gestellt, dass die physikalischen Gegebenheiten der Anschlussleitung, über die ein Endkundenstandort versorgt wird, dies ermöglichen. Auch in Vorleistungsverträgen alternativer Vorleistungsanbieter wird das Leistungsversprechen dahingehend eingeschränkt, dass die Übertragungsgeschwindigkeiten von den physischen Gegebenheiten der Netzinfrastruktur abhängen. Ist der Anbieter gegenüber dem Endkunden zur Minderung verpflichtet, ohne selbst entsprechende Ansprüche gegenüber dem Vorleistungserbringer zu haben, trägt er allein die finanziellen Folgen von technisch bedingten Leistungseinbußen. Dies kann sehr schnell dazu führen, dass das Produkt des Endkunden nicht mehr profitabel erbracht werden kann und für den Anbieter zu einem Verlustgeschäft wird. Damit führt die Regelung zu einer ungerechtfertigten Verlagerung wirtschaftlicher Risiken in die Sphäre der Diensteanbieter.

Zudem hat die von der BNetzA bereitgestellte Breitbandmessapplikation Ergebnisse geliefert, die zum Teil stark von der technisch gemessenen Bandbreite abweichen. Eine Abweichung muss daher auch mit anderen Messapplikationen überprüft und gegebenenfalls widerlegt werden können. Aber auch generell ist die Ermittlung der Bandbreite ungenau. Vom Kunden am Netzabschlusspunkt eingesetzte Telefonanlagen (diese sind vor allem im Kleingewerbe häufig im Einsatz) oder Router sowie die Inhouseverkabelung, welche nicht im Machtbereich des Anbieters des Telekommunikationsdienstes

liegt, können massiven Einfluss auf die Bandbreite und Qualität des Netzzugangs haben. Auch in diesen Fällen würde das Recht zur Minderung letztlich dazu führen, dass Kunden zwar ihre Entgeltzahlungen mindern können, die Anbieter aber keine Möglichkeit zur Nachbesserung haben.

Aus diesen Gründen spricht sich Telefónica dafür aus, dass in § 57 Abs. 4 enthaltene Minderungsrecht zu streichen. Zum einen entspricht eine solche Regelung nicht den Vorgaben des EECC, da dieser nur einen Bezug auf "die dem Verbraucher nach nationalem Recht, ..., zur Verfügung stehen." (Artikel 105 Abs. 5 EECC) fordert und keine Einführung neuer Rechtsbehelfe vorsieht. Darüber hinaus ist eine dauerhafte Minderung des Entgeltes im Rahmen eines Dienstleistungsvertrages auch im deutschen Recht nicht vorgesehen, da das von den Vertragsparteien intendierte Verhältnis zwischen Leistung und Gegenleistung erheblich verändert wird. Dies könnte insbesondere auf den Vorleistungsmärkten erhebliche Folgen haben.
Sollte das Minderungsrecht dennoch beibehalten werden, ist die Regelung dahingehend anzupassen, dass

- Im Falle einer Minderung auch der Anbieter den Vertrag kündigen kann
- Der Anbieter sich exkulpieren kann, wenn der Grund für die Leistungseinschränkung im Bereich eines Dritten liegen
- Die Möglichkeit besteht, bei Vorleistungsprodukten die Leistung nach Schaltung des Anschlusses festzulegen
- Mobilfunkleistungen vom Anwendungsbereich der Norm ausgenommen sind

Um Wiederholungen zu vermeiden, verweisen wir zudem auf die umfängliche Stellungnahme des VATM zu diesem Thema.

f. Kosten für Rufnummernmitnahme (§ 59 Abs. 3 TKG-E)

Der Diskussionsentwurf definiert in der Begründung zu § 59 Abs. 3 und 5 TKG-E den Begriff des „Anbieterwechsels" entgegen der derzeitigen Rechtslage und weitet damit die Regelungen in ihrer Anwendbarkeit aus, ohne dass dies im EECC vorgesehen ist.
Die Regelungen knüpfen beide – ebenso wie der heute geltende § 46 TKG – an den Begriff des „Anbieterwechsels" an. Die BNetzA hat sich u. a. im Beschluss BK2d-19/021 vom 26.09.2019 (Seite 9ff.) eingehend mit diesem Begriff auseinandergesetzt und kam zu dem Ergebnis, dass Voraussetzung für einen Anbieterwechsel der Wechsel des Kunden von einem Dienstleister zu einem anderen Dienstleister ist. Demgegenüber ist ein reiner Netzwechsel „bei Auslegung nach Wortsinn und Systematik sowie der Historie als auch nach Sinn und Zweck der Vorschrift und den europarechtlichen Grundlagen weder als ein Fall des Anbieterwechsels i.S.d. Vorschrift des § 46 Abs. 1 S. 1 TKG noch als ein sonstiger Wechselfall i.S.d. § 46 Abs. 5" (Beschluss BK2d-19/021 vom 26.09.2019 Ziffer 2.2.2) anzusehen.

Die Gesetzesbegründung des Diskussionsentwurfs scheint nun davon auszugehen, dass auch der reine Netzwechsel von der Regulierung erfasst sein soll. So wird in der Begründung zu Absatz 3 ausgeführt: „Eine Rufnummernübertragung ist somit auch unabhängig von einem Anbieterwechsel in Form eines reinen Netzwechsels möglich." und zu Absatz 5: „Es sind jedoch auch Rufnummernportierungen ohne Anbieterwechsel, also reine Netzwechsel, möglich, wenn der Kunde bei seinem bisherigen

Vertragspartner bleibt, dieser jedoch auf der Vorleistungsebene das Mobilfunknetz wechselt. […] Alle diese Sachverhalte unterfallen dieser Bestimmung."
Dies wäre eine Ausweitung des bisherigen Anwendungsbereichs, der vom Wortlaut des EECC nicht gedeckt ist und dem Ergebnis der detaillierten Auseinandersetzung der BNetzA mit diesem Thema konträr entgegensteht. Die vorstehend zitierten Sätze sollten daher aus der Gesetzesbegründung gestrichen werden.

g. Sperre bei Zahlungsverzug (§ 61 Abs. 4 TKG-E)

Das Recht der TK-Anbieter, Kunden wegen Zahlungsverzug den Telekommunikationsanschluss zu sperren, ist bereits nach dem jetzigen Recht (§ 45k TKG) gegenüber den allgemeinen Regelungen des bürgerlichen Rechts (§§ 273, 320 BGB) stark eingeschränkt. So dürfen u.a. bestrittene Forderungen grundsätzlich nicht berücksichtigt werden, der Zahlungsverzug muss mindestens 75€ betragen und die Sperre muss mit einem Vorlauf von zwei Wochen angekündigt werden. In § 61 Abs. 4 TKG-E wird die Möglichkeit zur Sperre wegen Zahlungsverzugs nun nochmals erheblich eingeschränkt.

Hervorzuheben ist zum einen die Nichtanrechenbarkeit der Grundentgelte bei der Berechnung der Verzugsschwelle, die sich in der Gesetzesbegründung findet. Bei der Berechnung der Verzugsschwelle sollen danach nur Forderungen für Verbindungsleistungen, nicht aber „Grundgebühren" einbezogen werden dürfen. Da es inzwischen Marktüblich ist, dass beinahe sämtliche TK-Leistungen durch Flatrates oder Pakete abgedeckt sind, fallen bei normaler Nutzung im Prinzip keine Verbindungsentgelte mehr an. Dies gilt weitgehend auch für die Nutzung im EU-Ausland. Damit bleiben von vorne herein nahezu sämtliche Entgeltforderungen unberücksichtigt.

Zum anderen ist die im Regierungsentwurf geplante Anhebung der Sperrgrenze von 75€ auf 150€ hervorzuheben, die in der Gesetzesbegründung mit der Ausweitung des Anwendungsbereichs der Vorschrift auf Internetzugangsdienste begründet wird. Dies überzeugt aus zwei Gründen nicht: Zum einen weil Internetdienste praktisch ausschließlich verbrauchunabhängig bepreist werden (z.B. Flatrate/ Volumenpaket) und daher verbrauchsabhängige Kosten (die allein berücksichtigt werden sollen) überhaupt nicht anfallen. Zum anderen deshalb, weil es marktüblich ist, dass im Basispreis nahezu alle Tarife Sprach- und Internetleitungen enthalten sind, und sich deshalb zumeist nicht einmal eine Steigerung der verbrauchsunabhängigen Preise ergibt. Tatsächlich würde die Preisentwicklung im TK-Bereich in den vergangenen Jahren eher eine Absenkung der Verzugsschwelle nahelegen. So sind beispielsweise ausweislich des Verbraucherpreiseindex des Statistischen Bundesamtes die Kosten für Mobilfunkleistung im Zeitraum 2015 bis 2020 um 5,5% gesunken.

Damit werden die Anbieter von TK-Diensten durch die sektorspezifische Regelung nochmals deutlich schlechter gestellt als andere Branchen und als nach den allgemeinen zivilrechtlichen Grundsätzen. Faktisch wäre eine Sperre unter den Voraussetzungen des § 59 Abs. 4 TKG-E nicht mehr durchführbar und Anbieter werden gezwungen auch bei dauerhafter vollständiger und unbegründeter Zahlungsverweigerung des Verbrauchers immer weiter ihre Dienste zu erbringen. Zu befürchten sind deutlich höhere Zahlungsausfälle, die kaufmännisch über den Grundpreis auf alle Verbraucher umgelegt werden müssten. Zu befürchten ist aber auch ein Anstieg kostenträchtiger Inkasso- oder Gerichtsverfahren zur Beitreibung offener Forderungen, die säumige Kunden zusätzlich belasten würden. Die Regelungen sind insbesondere auch nicht erforderlich, um eine ungerechtfertigte Sperre von TK-Leitungen (Art. 88 Abs. 2 EECC) zu unterbinden. Denn sämtliche Rechnungsbeträge

(insbesondere auch für Drittanbieterdienste) die der Kunde beanstandet, müssen bereits nach jetziger Rechtslage für die Sperre unberücksichtigt bleiben. Die Neuregelungen privilegieren daher im wesentliche die Einstellung von Zahlungen für unstreitige TK-Forderungen wie z.B. Grundgebühren und damit Missbrauch durch unbegründete Zahlungsverweigerung. Die Regelung stellt damit einen weitgehenden Eingriff in die Handlungsfreiheit der TK-Unternehmen dar, an dessen Verhältnismäßigkeit diesseits erhebliche Zweifel bestehen.

2. Informationen über den Netzausbau

a. Zentrale Informationsstelle des Bundes (§ 77 Abs. 2 TKG-E)

Die zentrale Informationsstelle des Bundes (ZiB) sollte zwingend bei der Bundesnetzagentur angesiedelt werden. Die bisher im TKG-E vorgesehene Verortung beim Bundesministerium für Verkehr und digitale Infrastruktur mit der bloßen Möglichkeit, die Aufgaben der ZiB ganz oder teilweise zu übertragen, sollte durch eine direkte Aufgabenzuweisung an die Bundesnetzagentur ersetzt werden. Schon heute besteht eine ZiB, die gemäß § 77a der aktuellen Fassung des TKGs bei der Bundesnetzagentur angesiedelt ist. Es ist nicht ersichtlich, warum dies für die Zukunft anders geregelt werden sollte. Ein Übergang der Aufgaben der ZiB von der Bundesnetzagentur auf das BMVI würde zwangsläufig zu Reibungsverlusten führen und faktisch nur Zeit und Aufwand kosten, ohne einen Mehrwert zu liefern.

b. Informationen über künftigen Netzausbau (§ 80 Abs. 1 TKG-E)

Einen staatlichen Eingriff in die Planungsprozesse der privaten Mobilfunkunternehmen, wie er in § 80 Abs. 1 TKG-E vorgesehen ist, lehnt Telefónica grundsätzlich ab. Dies würde zu zusätzlicher Bürokratie und Personalaufwand bei den Telekommunikationsunternehmen führen, ohne erkennbaren Vorteil für den Netzausbau zu bieten. Belastbare Aussagen über die Ausbauplanungen bzw. den zeitlichen Verlauf von Ausbauprojekten sind häufig nicht möglich, weil für die Realisierung von Standorten, Zuwegungen, Anbindungen mit Strom und Glasfaser bzw. Richtfunk und die Errichtung von Basisstationen eine Vielzahl von Gewerken und Genehmigungsprozessen ineinandergreifen müssen. Insbesondere ist der im § 80 Abs. 1 TKGE-E vorgesehene Planungszeitraum von 24 Monaten ungeeignet und unverhältnismäßig, weil er weder den Planungszeiträumen der Mobilfunkwirtschaft noch den für die Investitionsplanung maßgeblichen Geschäftsjahren entspricht. Zur Realisierung von Förderprogrammen werden ohnehin Markterkundungsverfahren durchgeführt, mit denen die Ausbauplanung der Netzbetreiber für ein geografisch bestimmtes Gebiet abgefragt wird. Es besteht keinerlei erkennbarer Mehrwert der Regelung, die jedoch aufgrund des geplanten staatlichen Zugriffs auf schutzbedürftige Betriebs- und Geschäftsgeheimnisse der Unternehmen deutlich in deren Grundrechte eingreifen würden. Die Norm ist aufgrund ihrer Unverhältnismäßigkeit daher rundum abzulehnen und aus dem TKG-E zu löschen.

3. Frequenzordnung

a. Zugang für Behördenfunk BOS (Art. 9 TKMoG-E)

Der in Art. 9 TKMoG-E formulierte § 24 Abs. 1 des BDBOS-Gesetzes-E sieht vor, dass Unternehmen, die öffentliche Telekommunikationsleistungen anbieten, der Bundesanstalt auf deren Verlangen hin unverzüglich, spätestens aber drei Monate nach Zugang des Angebotsverlangens, ein annahmefähiges Angebot zur Erfüllung der Aufgaben der Bundesanstalt nach § 2 Absatz 1 für die Bereitstellung von Telekommunikationsleistungen zu unterbreiten haben. Telefónica steht einer solchen Festlegung kritisch gegenüber, wonach ein gesetzlicher Anspruch auf Mitnutzung der privatwirtschaftlich betriebenen Mobilfunknetzbetreiber für den Behördenfunk BOS geschaffen werden soll. Es erscheint insofern äußerst fragwürdig, wenn der Staat sich in seiner Rolle als Gesetzgeber einen Zugangsanspruch für seinen eigenen Bedarfsträger schaffen möchte. Dies kommt einer nachträglichen Entwertung getätigter Investitionen der Mobilfunknetzbetreiber und einer nachgelagerte Neudefinition von Auflagen einer Frequenzzuteilung gleich. Hinzu kommt, dass ein solcher Zugang negativen Einfluss auf die Versorgung der Bevölkerung mit hochbitratigem Mobilfunk haben könnte.

b. Ziele der Frequenzregulierung (§ 86 Abs. 2 TKG-E)

Vor dem Hintergrund der weiter steigenden wirtschaftlichen und gesellschaftlichen Bedeutung von Mobilfunk sollte aus Sicht von Telefónica in § 86 Abs. 2 TKG-E ein weiteres Regulierungsziel aufgenommen werden, welches festlegt, dass Frequenzbänder, die gemäß internationaler Standardisierung und Harmonisierung für den öffentlichen Mobilfunk gewidmet sind, in Deutschland auch ausschließlich für diesen Zweck bereitgestellt werden dürfen. Das steigende Bedürfnis der Bevölkerung und der Industrie, Anwendungen der drahtlosen Vernetzung zu nutzen, sollte nicht dadurch konterkariert werden, dass verfügbare Frequenzen, die gemäß internationaler Standardisierung für den öffentlichen Mobilfunk genutzt werden können, in Deutschland für andere Anwendung vergeben werden. Eine solche Verknappung von Mobilfunkfrequenzen, wie sie beispielsweise durch die exklusive Zuweisung von Mobilfunkspektrum für industrielle, lokale Anwendungen in Deutschland bereits geschehen ist, führt letztlich zu einer künstlichen Verknappung von Mobilfunkfrequenzen und hat zudem negative Auswirkungen auf die Leistungsfähigkeit und verfügbare Bandbreite der öffentlichen Mobilfunknetze. Der Mobilfunkmarkt am Standort Deutschland würde dadurch als im internationalen Vergleich zurückfallen.

Telefónica regt daher die Ergänzung eines § 86 Abs. 2 Nr. 9 an:

> Die Bundesregierung handelt bei der Verfolgung der in Absatz 1 genannten Ziele im Einklang mit § 195 und mit der Entscheidung Nr. 676/2002/EG, in dem sie unter anderem
> (…)
> *9. verfügbare Frequenzen, die gemäß internationaler Harmonisierung und Standardisierung dem öffentlichen Mobilfunk gewidmet sind, ausschließlich zur Nutzung durch den öffentlichen Mobilfunk bereitstellt.*

c. Bedarfsermittlung sollte gesetzlich geregelt werden (§ 90 Abs. 10 TKG-E)

§ 90 Abs. 9 TKG-E legt fest, dass die Bundesnetzagentur im Falle eines Bedarfsüberhangs ein Vergabeverfahren nach § 999 TKG-E anordnen kann. Das Bedarfsermittlungsverfahren, durch welches die Bundesnetzagentur regelmäßig feststellt, ob ein solcher Bedarfsüberhang besteht, ist gesetzlich jedoch nicht geregelt, sondern bisher nur durch die Rechtsprechung des Bundesverwaltungsgerichts in seinen Grundzügen definiert (z.B. BVerwG Urteil vom 22.06.2011, 6 C 3.10). Da ein Bedarfsüberhang unmittelbare Voraussetzung für die etwaige Anordnung eines Vergabeverfahrens ist und somit erhebliche Auswirkungen auf die Marktteilnehmer haben kann, sollten die Anforderungen an die Bedarfsmeldung aus Sicht von Telefónica gesetzlich geregelt werden. Nur die Bedarfsmeldung eines Bedarfsträgers, der von Anfang an die subjektiven Voraussetzungen für die Zuteilung von Frequenzen erfüllt, sollte im Rahmen der Bedarfsermittlung maßgeblich sein.

Telefónica regt daher die Ergänzung eines § 90 Abs. 10 an:

> *10. Die Feststellung, ob die Voraussetzungen für Abs. 9 gegeben sind, erfolgt auf Basis eines qualifizierten Bedarfsermittlungsverfahrens. Unternehmen müssen im Rahmen eines solchen qualifizierten Bedarfsermittlungsverfahrens daher die subjektiven, fachlichen und sachlichen Anforderungen gemäß § 99 Abs. 4 Nr. 1 erfüllen.*

d. Befristung und Verlängerung der Frequenzzuteilung (§ 91 TKG-E)

aa. Dauer der Zuteilung

Frequenznutzungsrechte für drahtlose Breitbanddienste sollten zukünftig grundsätzlich immer für einen Zeitraum von mindestens 20 Jahren bereitgestellt werden, damit künftig Verlängerungen von Frequenznutzungsrechten, wie sie in § 91 Abs. 2, Abs. 3 geregelt sind, gar nicht mehr erforderlich sind.

Telefónica regt daher folgenden Änderung in § 91 Abs. 3 Satz 1 an:

> *Harmonisierte Frequenzen für drahtlose Breitbandnetze und –dienste werden für mindestens 20 Jahre zugeteilt bzw. entsprechend verlängert.*

bb. Ausgestaltung der Verlängerung

In § 91 Abs. 3 S. 4 TKG-E wird darauf hingewiesen, die Zuteilung harmonisierter Frequenzen für drahtlose Breitbanddienste zu verlängern, *damit der Regelungsrahmen für Investitionen in Netzinfrastrukturen für die Nutzung solcher Frequenzen während eines Zeitraums von mindestens 20 Jahren für die Inhaber der Frequenznutzungsrechte vorhersehbar ist*. Als Grund dafür wird in der Gesetzesbegründung darauf hingewiesen, dass eine Verlängerung der Zuteilung Planungssicherheit über mindestens 20 Jahre gewähren soll. Abs. 3 S. 5 stellt sodann klar, dass § 91 Abs. 2 davon unberührt bleibt. Dieser sieht wiederum vor, dass S. 3 unberührt bleibt, ohne aber direkt zu erwähnen, ob denn nun wirklich S. 3 von § 91 Abs. 2 gemeint ist. Wir unterstellen an dieser Stelle, dass es so ist. § 91 Abs. 2 S. 3 wiederum verweist auf eine entsprechende Anwendung von § 90 Abs. 9, welcher die Anordnung eines Vergabeverfahrens vorsieht, wenn für Frequenzzuteilungen nicht in ausreichendem Umfang verfügbare Frequenzen vorhanden oder für bestimmte Frequenzen mehrere Anträge gestellt sind. Unabhängig von der Unübersichtlichkeit dieser gesetzlichen Systematik (zu allem Überfluss wird in § 91 Abs. 2 S. 3 auch noch auf § 89 Abs. 9 S. 1 verwiesen, den es überhaupt nicht gibt) würde die

Verlängerung nach § 91 Abs. 2 TKG-E in Ansehung des in Spruchpraxis der Bundesnetzagentur faktisch immer bestehenden „Vorrangs des Vergabeverfahrens“ prinzipiell immer leerlaufen. Um dem entgegenzuwirken, sollten Frequenzen, die für einen kürzeren Zeitraum als 20 Jahre vergeben wurden auf Antrag ohne weitere Voraussetzungen auf eine Gesamtlaufzeit von mindestens 20 Jahren verlängert werden, selbst wenn die Voraussetzungen für die Anordnung eines Vergabeverfahrens gem. § 90 Abs. 9 TKG-E vorliegen. Jedenfalls darf es nicht Voraussetzung für eine Verlängerung sein, dass in der Zuteilung die Anforderungen des § 98 Abs.1 Ziff. 2 TKG-E erfüllt sind, da andernfalls die Möglichkeit einer Verlängerung von bereits vor Inkrafttreten dieses Gesetzes zugeteilten Frequenzen ausgeschlossen wäre. Zudem zementiert der bisher faktisch bestehende Regelfall eines Vergabeverfahrens in § 90 Abs. 9 TKG-E in Verbindung mit der Vorprägung auf die Versteigerung gem. § 99 Abs. 2 TKG-E permanente Planungsunsicherheit bei den Zuteilungsnehmern zugeteilter Frequenzen. Der Erwägungsgrund in der Gesetzesbegründung zu § 91 Abs. 3, nämlich Gewährung von Planungssicherheit für mindestens 20 Jahre, wird dadurch unterlaufen.

Telefónica regt aus diesen Gründen an, die Regelung in § 91 Abs. 3 ab S. 3 folgend auszugestalten:

> *(S. 3) Die Zuteilung ist auf Antrag bis zu einer Gesamtdauer von 20 Jahren zu verlängern. (S. 4) § 90 Abs. 9 TKG-E findet im Falle des § 91 Abs. 3 S. 3 TKG-E keine Anwendung. (S. 5) Über diesen Zeitraum hinaus ist die Zuteilung angemessen zu verlängern, damit der Regelungsrahmen für Investitionen in Netzinfrastrukturen für die Nutzung solcher Frequenzen für die Inhaber der Frequenznutzungsrechte vorhersehbar ist. (S.6) § 90 Abs. 9 TKG-E findet im Falle des § 91 Abs. 3 S. 5 TKG-E dieses Absatzes nur dann Anwendung, wenn besondere, überwiegende, schwerwiegende Gründe für ein Vergabeverfahren sprechen und ein Vergabeverfahren für den Zuteilungsnehmer nicht unzumutbar ist. (S.7) Die allgemeinen Kriterien der Verlängerung beziehen sich auf: […]*

Zusätzlich sollte folgender § 91 Abs. 5 TKG-E eingefügt werden:

> *(5) § 99 Abs. 2 S. 1 TKG-E findet auf § 91 TKG-E keine Anwendung.*

Als Alternative empfiehlt sich auch eine komplette Streichung von § 99 Abs. 2 S.1 TKG-E (siehe auch unten).

Klarstellend sollte in diesem Zusammenhang auch § 90 Abs. 9 TKG-E wie folgt ergänzt werden:

> *(9) Sind für Frequenzzuteilungen nicht in ausreichendem Umfang verfügbare Frequenzen vorhanden oder sind für bestimmte Frequenzen mehrere Anträge gestellt, kann die Bundesnetzagentur vorbehaltlich der Regelungen in § 91 TKG-E anordnen, dass der Zuteilung der Frequenzen ein Vergabeverfahren nach § 99 voranzugehen hat. Die Voraussetzungen einer Einzelzuteilung nach Absatz 5 bleiben hiervon unberührt. Vor der Entscheidung sind die betroffenen Kreise anzuhören. Die Entscheidung der Bundesnetzagentur ist zu veröffentlichen.*

e. Nachträgliche Änderung von Nebenbestimmungen der Frequenzzuteilung (§ 98 Abs. 2 Nr. 2 TKG-E)

§ 98 Abs. 2 Nr. 2 TKG-E stellt die überarbeitete Fassung des § 60 Abs. 2 S. 2 TKG (alt) dar. Dadurch sollen die Vorgaben des Art. 18 Abs. 1 EECC, welche durch Art 45 abs. 2 g) EECC eine Konkretisierung erfahren, umgesetzt werden. Gem. Art 45 abs. 2 g) EECC haben die Mitgliedstaaten u. a. Regeln für die Änderung von Funkfrequenznutzungsrechten anzuwenden, die klar und transparent festgelegt werden, um die Rechtssicherheit, Einheitlichkeit und Vorhersehbarkeit der Regulierung zu gewährleisten. § 98 Abs. 2 Nr. 2 TKG-E gewährleistet das nicht. Die Möglichkeit die Frequenz, Nebenstimmungen zur Frequenzzuteilung sowie Art und Umfang der Frequenznutzung unter Wahrung des Grundsatzes der Verhältnismäßigkeit nachträglich ändern zu können, gewährleistet weder Rechtssicherheit, Einheitlichkeit noch Vorhersehbarkeit der Regulierung. Der Regulierungsbehörde wird hierdurch die Möglichkeit eingeräumt, nachträgliche (belastende) Änderungen an bestandskräftigen Frequenzzuteilungen vorzunehmen ohne die Kriterien, unter denen das geschahen darf – so wie es nach dem aktuell gültigen § 60 Abs. 2 S. 2 TKG der Fall ist – zu bestimmen. Daher sollte an der alten Formulierung unter § 60 Abs. 2 S. 2 TKG (alt) festgehalten werden, zumal § 101 Abs. 1 TKG und § 49 Abs. 2 TKG der BNetzA bereits mannigfaltige Möglichkeiten einräumen, um nachträglich in bestehende Frequenzzuteilungen einzugreifen.

f. Vorprägung zu Gunsten der Versteigerung im Vergabeverfahren (§ 99 Abs. 2 TKG-E)

Im Bereich der Frequenzzuteilung wird mit dem vorliegenden Entwurf von § 99 Abs. 2 TKG-E die bisherige gesetzliche Vorprägung zugunsten von Versteigerungsverfahren zementiert, die regelmäßig zu Auktionen geführt hat. Diese Auktionen haben das Investitionsklima für Mobilfunkinfrastrukturen in Deutschland viele Jahre getrübt. Der EU-Kodex sieht hingegen ausdrücklich eine Öffnung für alternative Verfahren vor. Die Frequenzvergabe sollte sich daher strikt an den Regulierungszielen, wie der Beschleunigung des Ausbaus hochleistungsfähiger Telekommunikationsnetze oder der Gewährleistung der Versorgungssicherheit, ausrichten. Keinesfalls sollte im Vorgriff ein Verfahren als Regelverfahren der Frequenzvergabe festgelegt werden, sondern entsprechend dem EECC eine Öffnung für andere Bereitstellungsformen umgesetzt werden. Die Ausschreibung oder die Versteigerung sind nicht per se vorzugswürdig.

Telefónica regt daher folgende Änderungen an in § 99 Abs. 2 den folgenden Satz zu streichen:

Grundsätzlich ist das in Absatz 5 geregelte Versteigerungsverfahren durchzuführen.

Die nachfolgenden Sätze von § 97 Abs. 2 TKG-E sollten entsprechend angepasst werden.

g. Zahlungsbedingungen

Die Zahlung von Entgelten für Frequenznutzungsrechte soll laut Art. 42 EECC an die tatsächliche Verfügbarkeit der Frequenzen gekoppelt werden („pay-when-available“). Diese sehr sinnvolle Regelung, um den investierenden Unternehmen nicht vorfristig finanzielle Mittel zu entziehen, wird im TKG-E bedauerlicher Weise nicht ausreichend umgesetzt. § 222 Abs. 3 ermächtigt zwar das BMWi im Einvernehmen mit weiteren Ressorts die Höhe der zu erhebenden Gebühren näher zu bestimmen und dabei auch eine bestimmte Zahlungsweise der Gebühren anzuordnen. Diese Regelung umfasst jedoch nur die Gebühren für die Zuteilung von Frequenzen und nicht die beispielsweise im Rahmen einer Auktion erzielten Erlöse. Sie bleibt damit hinter dem Regelungsbereich des Art. 42 EECC zurück.

Zudem handelt es sich um eine Kann-Regelung, die der klaren Vorprägung des EECC zu Gunsten des “pay-when available”- wie auch des “pay-as-you-use"-Prinzips nicht gerecht wird.

Es sollte daher ein neuer § 222 Abs. 4 eingefügt werden, der klarstellt, dass Frequenzzuteilungsgebühren sowie Zahlungsverpflichtungen aus Frequenzvergabeverfahren erst bei Verfügbarkeit der betroffenen Frequenzen fällig werden und zudem jährliche Ratenzahlungen über die Laufzeit der Zuteilung hinweg festgelegt werden sollen.

4. Marktregulierung

a. Zugangsverpflichtungen (§ 26 Abs. 2 TKG-E)

§ 26 Abs. 2 TKG-E regelt, dass bei der Prüfung der Auferlegung von marktmachtabhängigen Zugangsverpflichtungen auch abgeschlossene oder angebotene kommerzielle Zugangsvereinbarungen berücksichtigt werden sollen. Der Verweis auf angebotene Vereinbarungen führt jedoch zu erheblicher Planungsunsicherheit, da das Bestehen eines Angebots allein nichts darüber aussagt, inwiefern dieses aus Nachfragersicht kommerziell tragfähig ist und inwieweit damit die Entwicklung eines nachhaltig wettbewerbsorientierten Endkundenmarktes überhaupt gefördert würde. Die Vorlage eines Angebots allein kann daher keinesfalls ausschlaggebend sein. Maßgeblich ist einzig das Vorliegen einer konkreten kommerziellen Vereinbarung mit einem Nachfrager, die im Grundsatz auch auf andere Marktteilnehmer übertragbar ist. Der Verweis auf „künftig abgeschlossene Vereinbarungen” ist zudem auch nicht durch den Wortlaut des EECC abgedeckt.

b. Maßstäbe bei Entgeltgenehmigung (§ 39 Abs. 2 TKG-E)

Die neue Form des § 39 Abs. 2 TKG-E weicht die bisherige eindeutige Vorprägung zu Gunsten der Anwendung des KeL-Maßstabs auf und räumt der Bundesnetzagentur „ein weites Ermessen mit Blick auf die Wahl des Maßstabs“ ein. Damit fällt die jetzige Formulierung hinter die bestehende Regelung zurück, welche ein klares Regel-Ausnahmeverhältnis definiert. Letztlich führt dies zu Planungsunsicherheit für alle Marktbeteiligten und konterkariert zudem die im Gesetzesentwurf definierten Ausnahmetatbestände, beispielsweise für Netze mit sehr hoher Kapazität oder Wholesale-Only-Anbieter. So sollte bei Feststellung beträchtlicher Marktmacht die Auferlegung des ex-ante Entgeltmaßstabs weiterhin die Regel sein.

5. Recht auf Versorgung mit Telekommunikationsdiensten

Es ist zu begrüßen, dass in § 156 Abs. 2 TKG-E die Versorgung mit einem angemessenen Breitbangzugangsdienst vorgesehen ist. Dies entspricht den Vorgaben des Art. 84 Abs. 3 EECC. Soweit die Versorgung mit einer höheren Bandbreite oder Qualität verpflichtend werden soll, müsste diese Verpflichtung staatlich und nicht mittels eines Umlageverfahrens finanziert werden.

Die Versorgungspflicht stellt jedoch einen erheblichen Eingriff in den Wettbewerb auf dem Telekommunikationsmarkt dar, kann für die verpflichteten Unternehmen zu einer erheblichen Bindung von Unternehmensressourcen führen und letztlich deren Geschäftstätigkeit erheblich beeinträchtigen. Durch das Umlageverfahren belastet die Versorgungspflicht auch alle anderen Telekommunikationsunternehmen. Aus Sicht von Telefónica muss die Regelung zur Ermittlung einer

Unterversorgung (§ 156, 159 TKG-E) daher technologieneutral ausgestaltet sein. Alle Telekommunikationstechnologien müssen bei der Ermittlung der ausreichenden Versorgung mit einbezogen werden. Dies sollte insbesondere auch die Versorgung über Satellit und per Mobilfunk einbeziehen. Die Versorgungspflicht ist wie dargelegt eine erhebliche Beeinträchtigung für alle Telekommunikationsunternehmen und darf daher nur als letztes Mittel genutzt werden, wenn mit allen anderen technologischen Möglichkeiten keine ausreichende Versorgung erreicht werden kann.

Aus demselben Grund müssen vor einer Anordnung der Versorgungspflicht auch alle anderen Möglichkeiten der Förderungen des Netzausbaues zunächst ausgeschöpft werden. Es muss in diesem Zusammenhang immer der Vorrang der bestehenden Förderprogramme von Bund und Ländern gelten, da dieses Mittel die Telekommunikationsunternehmen weit weniger belastet.

Das vorgesehene Umlageverfahren ist sehr bürokratisch und wird die Verfahren zur Versorgungsverpflichtung erheblich verkomplizieren und verzögern. Im Übrigen wird die Umlage faktisch zu steigenden Endkundenpreisen oder zu sinkenden Umsätzen in der Telekommunikationsbranche führen. Dies wiederum hätte negativen Einfluss auf die Investitionsfähigkeit der Branche und könnte den Netzausbau insgesamt sogar verlangsamen. Vor diesem Hintergrund sprechen wir uns dafür aus, dass eine staatliche Finanzierung zumindest in dem TKG-E vorgesehen wird.
Im Übrigen verweisen wir im Einzelnen auch auf die Stellungnahme der Telekommunikationsverbände zu den Versorgungspflichten.

6. Wegerechte und Mitnutzung

Die Regelungen des Abschnitt 8 TKG-E, die sich mit den Wegerechten und den Zugang zu öffentlicher Infrastruktur für den Netzausbau befassen, begrüßt Telefónica grundsätzlich. Schon die bisherigen Regelungen hierzu aus §§ 68 ff. und 77a ff. TKG haben über die Jahre hinweg deutliche Verbesserungen für den praktischen Netzausbau gebracht. Kritisch bewertet Telefónica jedoch insgesamt, dass sämtliche Maßnahmen und Ansprüche, die im neuen Abschnitt 8 geregelt sind, lediglich zu Gunsten der Netze mit hoher Kapazität ausgestaltet sind. Dies würde explizit Mobilfunknetze, die nicht per se glasfaserbasiert sind, ausschließen. Daher regt Telefónica an, die Ansprüche des gesamten Abschnitt 8 auch auf drahtlose Breitbandnetze und –dienste im Sinne des § 3 Abs. 1 Nr. 11 TKG-E auszuweiten.

7. Angemessene Übergangsfristen notwendig

Für die Umsetzung der neuen Vorgaben des TKG-E ist eine angemessene Umsetzungsfrist von mindestens 12 Monaten ab Abschluss des Gesetzgebungsverfahrens zu gewähren.

Rechtlicher Ausgangspunkt ist der Beschluss des Bundesverfassungsgerichts vom 4. Mai 2012 (1 BvR 367/12) wonach Unternehmen mit der Implementierung von Gesetzen nicht vor deren Zustandekommen beginnen müssen.

Die Anwendung dieses Grundsatzes halten wir im vorliegenden Fall für essentiell. Bei der derzeitigen Entwurfsfassung des TKG-E können sich einzelnen Regelungen durch den Konsultationsprozess oder später im politischen Gesetzgebungsprozess ändern. Damit besteht für die Unternehmen keine hinreichende Sicherheit, welche Vorgaben umgesetzt werden müssen. Diese Sicherheit ist erst nach dem Erlass des Gesetzes gegeben.

Aus dem derzeitigen Entwurfsstand des Gesetzes ergibt sich unserer Ansicht nach zum Beispiel noch nicht, ob die Neuregelungen nur für Verträge gelten sollen, die nach dem Inkrafttreten des Gesetzes geschlossen wurden oder auch für Bestandsverträge. Diese Frage hat erhebliche Auswirkungen auf die Umsetzung. Gelten die Regeln nur für neu abgeschlossene Verträge, müssten nur die Vertragsgestaltung für die Zukunft angepasst werden. Bei einer Geltung für alle Verträge müssten alle Bestandsverträge analysiert und gegebenenfalls angepasst werden. Auch scheint immer noch nicht abschließend geklärt zu sein, wie die Regelung zur Mindestvertragslaufzeit ausgestaltet wird. Neben der rein technischen Umsetzung in Kundenmanagement- und Vertragsverwaltungssystemen, die beispielsweise bei der Umsetzung der Pflicht zur Tarifberatung nach § 55 Abs. III TKG-E erforderlich ist oder der Umsetzung der Informationspflichten in allen Vertriebskanälen (Onlineshop, Telesales, Point of Sales) müssen auch zahlreiche organisatorische Maßnahmen ergriffen werden. So muss beispielsweise das Personal in der Kundenbetreuung für die neuen gesetzlichen Regelungen geschult werden und für die Abwicklung neuer Prozesse wie die Tarifberatung muss ggfs. auch zusätzliches Personal angestellt werden.

Wir möchte in diesem Zusammenhang unterstreichen, dass die Forderung nach einer ausreichenden Umsetzungsfrist den tatsächlichen Gegebenheiten geschuldet ist. Wird mit der konkreten Umsetzung vor der Wirksamkeit des zugrundeliegenden Gesetzes begonnen, entstehen bei den Unternehmen erhebliche Kosten und Verzögerungen. Wenn auf Basis einer erwarteten Regelung der oben genannte Entwicklungsprozess gestartet wird und die Regelungen später geändert werden, muss der Umsetzungsprozess gestoppt und angepasst werden. Damit verzögert sich die Umsetzung und eine fristgerechte Einführung kann nicht gewährleistet werden. Ebenso ist es möglich, dass die geänderten Vorgaben nicht mehr berücksichtigt werden können. In diesem Fall würde die fristgemäße Umsetzung auf dem alten Entwurf des Gesetzes basieren und die neuen Änderungen nicht berücksichtigen. Anschließend müsste aufgrund der Endfassung des Gesetzes ein Änderungsprozess angestoßen werden, der erst Monate später umgesetzt werden kann.

8. Verfassungsgemäße Überleitungsvorschrift

Zusätzlich zu der angemessenen Umsetzungsfrist ist es rechtsstaatlich geboten, die Geltung der neuen EECC Regelungen ausschließlich auf neue abgeschlossene Verträge zu beziehen. Ansonsten würden die neuen Regelungen in bestehende Rechtsverhältnisse eingreifen. Die kommerziellen Voraussetzungen, unter denen die Parteien die bestehenden Verträge geschlossen haben, würden damit nachträglich und unzumutbar verändert. So hat die Dauer der initialen Laufzeit und der Vertragsverlängerung eine erhebliche kommerzielle Auswirkung auf das Entgelt. Ein nicht unerheblicher Anteil der Kosten eines Telekommunikationsvertrages fällt bei der Anbahnung und Einrichtung des Vertrages an. Diese Kosten werden nicht selten auf die gesamte vereinbarte Laufzeit verrechnet. Dies gilt insbesondere auch für Provisionen. Wenn die Vertragslaufzeit nachträglich angepasst wird, wird die vereinbarte kommerzielle Grundlage des Vertrages zerstört.

Dieses Vorgehen entspricht im Übrigen den üblichen Überleitungsregelungen für vertragsrelevante Regelungen gemäß Art. 229 des Einführungsgesetzes zum Bürgerlichen Gesetzbuch (EGBGB).

Ansprechpartner:
Philippe Gröschel, Head of Government Relations, philippe.groeschel@telefonica.com

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
19(4)749

STELLUNGNAHME

Berlin, 26. Februar 2021

Deutscher Industrie- und Handelskammertag

Gesetzentwurf der Bundesregierung: Entwurf eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (Zweites IT-Sicherheitsgesetz – IT-SiG 2.0)

Daten, Systeme und Infrastrukturen – die Digitalisierung insgesamt – werden immer wesentlicher für die Wettbewerbsfähigkeit und gar generell den Fortbestand von Unternehmen. Aufgrund der starken Abhängigkeit der gewerblichen Wirtschaft von sicheren digitalen Infrastrukturen und Anwendungen setzt sich der DIHK für geeignete Rahmenbedingungen ein, um die Daten- und Informationssicherheit in der Breite der Wirtschaft zu verbessern. Er nimmt wie folgt zu ausgewählten zentralen wirtschaftsbezogenen Aspekten des vorliegenden Entwurfes Stellung:

Unternehmen sind grundsätzlich selbst für das Handling der Risiken in ihrem eigenen Verantwortungsbereich verantwortlich. Jeder Unternehmer muss – im Rahmen der gesetzlichen Vorgaben – entscheiden, welche eigenen Daten, Informationen und Infrastrukturen besonders schützenswert sind und die erforderlichen Schutzmaßnahmen treffen. Unseren Erfahrungen nach haben Unternehmen in den letzten Jahren in der Regel entsprechende technische und organisatorische Vorkehrungen getroffen. Individuelle Datensicherheit ist zugleich aber auch ein Beitrag zur gemeinschaftlichen Resilienz. Wo besondere Risiken bestehen, müssen andere Marktteilnehmer durch spezielle rechtliche Vorgaben geschützt werden – so geschehen etwa mit den Regelungen des ersten IT-Sicherheitsgesetzes zu kritischen Infrastrukturen.

Der Gesetzgeber hat mit dem ersten IT-Sicherheitsgesetz Meldepflichten für IT-Sicherheitsvorfälle und Mindestsicherheitsstandards für die Betreiber kritischer Infrastrukturen wie Energie, Wasser, Gesundheit oder Telekommunikation eingeführt, die erst nach und nach in der Umsetzung ankommen. Mit dem vorliegenden Entwurf eines IT-Sicherheitsgesetzes 2.0 werden zusätzliche gesetzliche Anforderungen an weitere Unternehmen im besonderen öffentlichen Interesse vorgesehen, bevor evaluiert wurde, inwiefern die bisherigen Verpflichtungen zu einem höheren IT-Sicherheitsniveau beitragen. Wir empfehlen, bei künftigen Gesetzgebungsvorhaben konkrete Evaluierungen vorzusehen und diese verbindlich in den Gesetzgebungsprozess einfließen zu lassen, um auf Basis dieser Erkenntnisse eventuellen zusätzlichen Regelungsbedarf der Unternehmensrealität anzupassen. Bei der Ausweitung gesetzlicher Vorgaben sollten konkrete Umsetzungserfordernisse in den Unternehmen von Beginn an in die Betrachtungen einbezogen werden. Eine solche vollzugssensitive Regulierung sollte von vornherein das Verhältnis der damit

DIHK | **Deutscher Industrie- und Handelskammertag e.V.**
Besucheranschrift: Breite Straße 29 | 10178 Berlin-Mitte | Postanschrift: DIHK | 11052 Berlin

Tel. 030-20308-0 | Fax 030-20308-1000 | Internet: www.dihk.de

verbundenen Belastungen und den konkreten Nutzen einer Regelung für die Unternehmen in den Blick nehmen.

Dem vorliegenden Entwurf zufolge entsteht der Wirtschaft für die Erfüllung der im Gesetz vorgesehenen zusätzlichen Aufgaben ein einmaliger Aufwand in Höhe von ca. 40.000 Euro sowie laufende Aufwände in Höhe von rund 21 Millionen Euro. Die Ermittlung des Erfüllungsaufwands für die Wirtschaft ist laut Entwurf „nur unter hoher Unsicherheit quantifizierbar“ und sind „somit als Mindestwerte zu verstehen“. Der tatsächliche Aufwand in den Unternehmen dürfte wesentlich höher liegen, so sind beispielsweise etwaige Folgekosten nicht erfasst, die in der Anwendung des Gesetzes entstehen, etwa bei einer möglichen Rückbauanordnung. Insbesondere vor diesem Hintergrund sollte den betroffenen Unternehmen durch das Gesetzesvorhaben nicht nur Aufwand, sondern vor allem ein unmittelbarer Gewinn an IT-Sicherheit entstehen. Ein konkreter Mehrwert durch die Erfüllung zusätzlicher Verpflichtungen, insbes. Meldepflichten, sollte im Gesetzentwurf deutlicher herausgearbeitet werden. Hilfreich für die Unternehmen könnte beispielsweise ein aktuelles Lagebild inkl. branchenspezifischer Handlungsempfehlungen sein, aber auch Unterstützung durch die Mobile Incident Response Teams.

Im Fokus des Gesetzentwurfs stehen vor allem (End)Nutzer, große Unternehmen sowie Unternehmen mit kritischer Infrastruktur. Wünschenswert wäre eine stärkere Fokussierung auch auf pragmatische Unterstützungsleistungen – nicht zusätzliche regulatorische Belastungen – insbesondere kleinerer und mittlerer Unternehmen bei der Erhöhung ihrer Daten- und Informationssicherheit. Diese sollten als relevante Zielgruppe stärker benannt werden, ggf. wäre bei den betreffenden Regelungen der Begriff „Anwender“ statt „Verbraucher“ treffender. Die folgenden Ausführungen nehmen daher die Auswirkungen des Entwurfes auf Anwender im Sinne von Unternehmen in den Fokus und beziehen sich nicht auf den Verbraucherbegriff im Sinne des BGB. Sofern kleine und mittlere Unternehmen in den Anwendungsbereich des Gesetzes fallen, sind selbst die o. g. Aufwände nicht darstellbar. Hier ist mehr Augenmaß bei der Gesetzgebung und eine Orientierung an den unternehmerischen Realitäten gefragt.

Insgesamt ist ein systematisches, gesamtheitliches Vorgehen zum Schutz der Wirtschaft erforderlich. Dieses sollte darauf ausgerichtet sein, Daten- und Informationssicherheit in der Unternehmerschaft im Sinne eines breiten Resilienzstandards umzusetzen. Das Sicherheitsniveau sollte durch verschiedene Maßnahmen (rechtliche Vorgaben, Informations- und Unterstützungsleistungen, Förderung etc.) schrittweise erhöht werden. Erforderlich dafür ist ein übergreifendes Gesamtkonzept, das das Zusammenspiel freiwilliger und verpflichtender Vorhaben transparent macht, Lösungen im europäischen Kontext und einen konkreten Umsetzungsplan beinhaltet. Das IT-Sicherheitsgesetz ist ein Teil dieses Gesamtkonzepts und sollte eine entsprechende Einordnung finden. Insbesondere weisen wir darauf hin, dass zentrale Begriffe des Entwurfs im Einklang mit europäischen Regelungen erfolgen sollten, – insbes. zur europäischen Richtlinie zur Erhöhung der Netz- und Informationssicherheit (sog. NIS-Richtlinie), die gerade überarbeitet wird – um Rechtsunsicherheiten für die Unternehmen zu vermeiden.

Im Einzelnen:

Ausweitung von Pflichten sollte mit konkreten Sicherheitsgewinnen einhergehen

Für die Betreiber von kritischen Infrastrukturen bestehende Meldepflichten und Verpflichtungen zur Gewährleistung eines Mindestsicherheitsstandards sollen auf weitere Teile der Wirtschaft ausgeweitet werden. Hierunter fallen insbes. solche Unternehmen, an deren Funktionsfähigkeit ein „besonderes öffentliches Interesse“ besteht, worunter nach § 2 Absatz 14 Nr. 2 BSIG-E unter anderem Unternehmen zu verstehen sind, die nach ihrer inländischen Wertschöpfung zu den größten Unternehmen in Deutschland gehören und daher von erheblicher volkswirtschaftlicher Bedeutung für die Bundesrepublik Deutschland sind. Entsprechende Unternehmen sollen durch Rechtsverordnung bestimmt werden, in der „abstrakt-generelle Kriterien verbindlich vorgegeben“ werden, „nach denen Unternehmen selbst feststellen können, ob sie Unternehmen im besonderen öffentlichen Interesse“ sind. Dabei soll man sich am Gutachten der Monopolkommission orientieren, in dem „die einhundert größten Unternehmen Deutschlands nach inländischer Wertschöpfung ermittelt“ werden.

Aus Gründen der Sachnähe und Flexibilität ist es zwar sinnvoll, nicht jedes kleinste Detail durch Gesetz zu regeln, Unternehmen benötigen aber frühzeitig Rechtssicherheit darüber, wen genau die neuen Regelungen betreffen und was sie zu tun haben. Mithin erscheinen die Maßstäbe zur Bestimmung des Adressatenkreises zu unbestimmt – auf europäischer Ebene sind keine vergleichbaren Regelungen im Rahmen der NIS-Richtlinie vorgesehen. Doppelregulierungen und Widersprüche sind zu vermeiden. Um die Bürokratielast nicht unnötig zu vergrößern, sollte die Ausweitung des Kreises der Unternehmen, denen die aufwändigen Zusatzpflichten auferlegt werden, auf ein notwendiges Maß begrenzt sein.

Die Einbeziehung von wichtigen Unternehmen über den KRITIS-Kernbereich hinaus ist für diese mit Aufwand verbunden, der laut Entwurf nur „unter hoher Unsicherheit quantifizierbar“ ist. Für die betroffenen Unternehmen sollte aber nicht nur Aufwand, sondern vor allem ein unmittelbarer Gewinn an IT-Sicherheit entstehen, wenn sie zusätzliche Verpflichtungen erfüllen müssen. Ein solcher könnte sich etwa durch ein aktuelles Lagebild mit entsprechenden Handlungsempfehlungen oder durch Unterstützung im Schadensfall ergeben. Dafür sollte sichergestellt sein, dass auch das entsprechende Fachpersonal im BSI verfügbar ist.

Mehr Kompetenzen des BSI nur in Verbindung mit mehr Transparenz und konkretem Mehrwert für die Unternehmen

Das BSI erhält zahlreiche zusätzliche Befugnisse. Eingeführt werden soll eine Bestandsdaten-auskunft für Anbieter von Telekommunikationsdiensten. Diese Informationen sollen verwendet werden, um Betreiber kritischer Infrastrukturen, Unternehmen im besonderen öffentlichen Interesse und Anbieter digitaler Dienste über die dazugehörigen Cyber-Angriffe zu informieren und bei der Angriffsabwehr zu unterstützen. Darüber hinaus kann das BSI bei den genannten Institutionen aktive Detektionsmaßnahmen durchführen sowie generell Produkte und Systeme untersuchen und

die Ergebnisse veröffentlichen. Auch dafür müssen die verpflichteten Unternehmen Informationen bereitstellen. Zur Gefahrenabwehr soll nach dem Entwurf das BSI Maßnahmen für Diensteanbieter anordnen können. Es wird eine Registrierungspflicht für Betreiber kritischer Infrastrukturen und für Unternehmen im besonderen öffentlichen Interesse eingeführt, und das BSI soll Cybersicherheitszertifikate für Systeme, Komponenten und Produkte ausstellen, wofür es vorab den sog. Stand der Technik festlegen soll.

Die Entwicklung und Veröffentlichung von sicherheitstechnischen Anforderungen an IT-Produkte durch das BSI darf nicht in einen nationalen Alleingang münden, und es sollten keine Parallelstrukturen aufgebaut werden. Der Stand der Technik sollte wie bisher auf Basis anerkannter Normen und Standards ausgelegt werden, an deren Erarbeitung die betroffenen Unternehmen und Normungsorganisationen beteiligt sind.

Angesichts des geplanten umfangreichen Ausbaus der Aufgaben und Kompetenzen des BSI stellt sich die Frage nach der Erhöhung der Akzeptanz für diese zusätzlichen Befugnisse, insbesondere vor dem Hintergrund der geplanten zusätzlichen Detektions-, Kontroll- und Anordnungsbefugnisse und der engen Zusammenarbeit zwischen BSI und Sicherheitsbehörden. Auf die IT-Sicherheit von Unternehmen wirkt sich insbesondere der Umstand aus, dass das BMI mit dem BSI eine Behörde beheimatet, die IT-Sicherheit fördern soll, und zugleich auch Behörden, für deren Arbeit auch IT-Schwachstellen genutzt werden. Zugleich ist der staatliche Umgang mit Schwachstellen in Hard- und Software ungeklärt. Viele Unternehmen fragen sich, inwieweit das BSI aufgedeckte Schwachstellen an andere Sicherheitsbehörden weiterleitet, statt auf die Schließung dieser Lücken hinzuwirken, die auch von anderen Staaten und organisierter Kriminalität genutzt werden und damit erhebliche Schäden bei betroffenen Unternehmen verursachen können.

Das in § 7 Abs. 2 BSIG-E formulierte eigene Ermessen als Grundlage, Sicherheitslücken zu publizieren, erscheint insofern zu unspezifisch. Hier sollte klargestellt werden, dass das BSI derartiges Wissen und auch darüber hinaus bekanntgewordene Erkenntnisse mit der Wirtschaft teilen muss, um ein schnelles und sachgerechtes Schließen von Sicherheitslücken auch in anderen Bereichen kritischer Infrastrukturen zu ermöglichen. Insbesondere darf das BSI-Gesetz kein Einfallstor für die Aufweichung von Verschlüsselung durch sog. Backdoors werden.

Eine getrennte Fachaufsicht über defensive (BSI) und offensive Sicherheitsbehörden könnte zudem ein Mindestmaß an Grundvertrauen in der Wirtschaft schaffen. Von einer ernsthaften Befassung der Bundesregierung mit diesem Thema würde die Cyber- und IT-Sicherheit der Unternehmen profitieren. Denn das BSI kann seinem Auftrag – die IT-Systeme in Deutschland sicherer zu machen – nur in vertrauensvoller Zusammenarbeit mit den Marktakteuren effektiv nachkommen.

Das Bestandsdatenauskunftsverlangen richtet sich an denjenigen, „der geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt". Damit könnte jeder Anbieter umfasst sein, gleich welcher Größenordnung. Zudem wird aus dem Entwurf nicht deutlich, wie Diensteanbieter sich gegen Anordnungen des BSI zu Umleitungen des Datenverkehrs an eine vom BSI benannte Anschlusskennung (sog. Sinkhole-Server zur Verminderung der Gefahren von

Botnetzen) verwehren können. Dies scheint eine unzulässige Vermengung der BSI-Anordnungen zur allgemeinen Sicherheitserhöhung mit Verfahren der Strafverfolgung.

Für Betreiber Kritischer Infrastrukturen und Unternehmen im besonderen öffentlichen Interesse besteht künftig eine Registrierungspflicht beim BSI – unabhängig von der bereits bestehenden Regstrierungspflicht für eine Kontaktstelle. Es ist für Unternehmer bereits jetzt schwierig, den Überblick zu behalten, wo sie sich überall registrieren oder eintragen lassen müssen. Wird eine Registrierung nicht oder nicht rechtzeitig vorgenommen, handelt es sich um eine Ordnungswidrigkeit, die mit einer Geldbuße geahndet werden kann. Im Hinblick auf eine ebenfalls geplante Registrierungspflicht im Rahmen der NIS-Richtlinie sollte von vorn herein sichergestellt werden, dass nicht mit Inkrafttreten der NIS-Richtlinie erneute Registrierungspflichten auf die Unternehmen zukommen.

Das BSI soll zentrale Meldestelle für die Sicherheit in der Informationstechnik werden. Hierfür soll es Informationen über Sicherheitsrisiken in der Informationstechnik (z. B. zu Sicherheitslücken, Schadprogrammen, Angriffen) entgegennehmen, diese auswerten und verarbeiten. Die Verarbeitung umfasst die Weitergabe unternehmerischer Daten durch die Information Dritter, die Warnung der Öffentlichkeit und die Unterrichtung von Betreibern Kritischer Infrastrukturen. Es sollte klargestellt werden, dass bei Meldungen generell bereits etablierte Meldewege genutzt werden und kein zusätzlicher Kanal bedient werden muss. Zudem bedarf es einer Konkretisierung des dadurch für die Unternehmen entstehenden Mehrwerts – detailliertes Lagebild und Handlungsempfehlungen.

Geprüft werden sollte deshalb auch, inwieweit die erlangten Informationen über den Kreis der Betreiber kritischer Infrastrukturen, Unternehmen im besonderen öffentlichen Interesse und Anbieter digitaler Dienste hinaus auch anderen betroffenen Unternehmen möglichst zielgenau zur Verfügung gestellt werden können, etwa den Partnern der Allianz für Cybersicherheit. Eine Aufbereitung der Informationen je nach Adressatenkreis ist dabei notwendig. Meldungen zu Schwachstellen sind den betroffenen Unternehmen zuerst mitzuteilen, so dass diese die Möglichkeit haben, die Sicherheitslücken zu schließen. Sie dürfen keinesfalls für die Tätigkeit anderer staatlicher Akteure offengehalten bzw. genutzt werden.

Insgesamt sollte bei den einzelnen Verpflichtungen stärker darauf geachtet werden, inwieweit die Maßnahmen von den Unternehmen, insbesondere auch von kleinen und mittleren Unternehmen, aus wirtschaftlichen Erwägungen leistbar sind und mit welchem zusätzlichen Sicherheitsgewinn jeweils faktisch zu rechnen wäre. Entsprechende Eingrenzungen des Anwendungsbereichs scheinen insbesondere mit Blick auf die angepassten Bußgeldvorschriften erforderlich.

Infrastrukturen innovationsoffen und sicher gestalten – geeignete Rahmenbedingungen auf europäischer Ebene schaffen

Eine zentrale Regelung des Entwurfs betrifft den Einsatz besonders kritischer Komponenten im Bereich der kritischen Infrastrukturen. Dieser soll künftig unter bestimmten Voraussetzungen

untersagt werden können. Vorgesehen ist ein mehrstufiges Verfahren, in dem vor Einsatz der Komponenten die technische Zuverlässigkeit geprüft, zertifiziert und von den Betreibern eine Garantieerklärung der Hersteller der kritischen Komponenten vorgelegt werden muss. Anschließend erfolgt eine Prüfung, ob dem Einsatz der Komponenten überwiegende öffentliche Interessen, insbesondere sicherheitspolitische Belange entgegenstehen. Darüber entscheiden die betreffenden Ressorts der Bundesregierung.

Die Sicherheit von Daten und Informationen aller Anwenderunternehmen hängt davon ab, ob (Vor)Produkte, Komponenten und Infrastrukturen sicher sind. Spezifische IT-Sicherheits-Vorgaben sind für sicherheitsrelevante Produktkategorien erforderlich. Mit einer entsprechenden Regelung kann mehr Transparenz geschaffen und den Anwenderunternehmen die Nutzung von geprüft sicheren Infrastrukturen zumindest erleichtert werden. Auf der anderen Seite werden den Betreibern kritischer Infrastrukturen wesentliche Belastungen auferlegt – von der Einholung der Garantieerklärung für kritische Komponenten bis hin zum Umbau der Systeme bei einer eventuellen Untersagung eines Komponenteneinsatzes, ohne dass im Entwurf Schadensersatzleistungen oder Umsetzungszeiträume geregelt wären.

Bei einem solch vielschichtigen Problem wird eine rein nationale Lösung langfristig nicht weiterhelfen. Fraglich ist, ob ein nationales Vorpreschen hier nicht allein nationale Anbieter benachteiligt. Innerhalb der EU sollten keine künstlichen Marktverzerrungen kreiert werden. Die Bundesregierung ist deshalb gefordert, gemeinsam mit den anderen EU-Mitgliedstaaten eine nachhaltige, zukunftsoffene Lösung auf europäischer Ebene zu finden. Mittelfristig sollte die EU die Rahmenbedingungen dafür schaffen, die europäischen Kräfte in Hochtechnologiebereichen und kritischen Infrastrukturen besser zu bündeln, und in diesem Zuge die Wettbewerbsfähigkeit und digitale Sicherheit der gewerblichen Wirtschaft in einer digitalisierten Welt auch europaweit zu gewährleisten.

Eine Erklärung des Herstellers über seine Vertrauenswürdigkeit gegenüber dem Betreiber der Kritischen Infrastruktur (Garantieerklärung), die sich über die gesamte Lieferkette des Herstellers erstreckt, ist im Zeitalter von internationalen Zulieferern und Open-Source-Software kaum verbindlich leistbar und auch nicht durch den Betreiber überprüfbar. Es ist nicht zu erwarten, dass einzelne Hersteller eine solche Erklärung nicht abgeben würden. Von daher erscheint die Aussagekraft einer solchen von vorn herein sehr beschränkt. Der Fokus sollte vielmehr auf Prozesse zur Stärkung der Sicherheit gelegt werden.

Ferner bedeutet eine drohende Untersagungsanordnung für den Betreiber ein nahezu unbeherrschbares über den gesamten Lebenszyklus einer Komponente andauerndes Risiko. Dadurch erfolgt ein massiver nachträglicher Eingriff in bereits in der Vergangenheit auf Basis geltenden Rechts getroffene Investitionsentscheidungen sowie in grundgesetzlich geschützte Rechtspositionen. Im Falle einer Untersagung des Einsatzes kritischer Komponenten nicht vertrauenswürdiger Hersteller sollten zumindest bestandssichernde Regelungen zur Aufrechterhaltung der kritischen Geschäftsprozesse getroffen werden.

Zudem ist eine Definition materiell nachprüfbarer Gründe im Gesetz erforderlich, die der Vertrauenswürdigkeit entgegenstehen. Eine Untersagung muss für den Betreiber nachvollziehbar und materiell begründbar sein. Dabei sind weitere Wechselwirkungen (u.a. Ausbauverpflichtungen, Betriebskontinuität) zu berücksichtigen, um im Einvernehmen mit den Verpflichteten die Funktionsfähigkeit der Infrastrukturen als solcher zu gewährleisten.

Dies gilt insbesondere für bereits im Einsatz befindliche kritische Komponenten. Eine grundlegende Definition kritischer Kernkomponenten leistet der Gesetzentwurf indes nicht. Die Entscheidung, welche Komponenten dem Regime des IT-Sicherheitsgesetzes unterworfen werden, obläge damit allein dem Verordnungsgeber. Den möglichen, insbesondere erheblichen wirtschaftlichen Folgen für die Betreiber wird dies nicht gerecht, so dass eine Konkretisierung im Gesetz erforderlich ist.

Der neue § 10 Abs. 6 BSIG-E sieht vor, dass das BMI unter Beteiligung von Verbänden und des BMWi durch Rechtsverordnung die Offenlegung von Schnittstellen und die Einhaltung etablierter technischer Standards bestimmen kann. Diese allgemeine Anordnungsbefugnis zur Offenlegung von Schnittstellen, Einhaltung etablierter technischer Standards und Interoperabilität wird in der Unternehmerschaft kontrovers diskutiert. Auf der einen Seite wird gewürdigt, dass das Potenzial von Interoperabilität zur langfristigen Steigerung der IT-Sicherheit und digitalen Souveränität im Gesetzestext explizit aufgeführt wird. Andere Marktvertreter hingegen führen an, dass durch die Offenlegung von Schnittstellen zusätzliche Sicherheitsrisiken geschaffen werden, weil sensible, für den Schutz der Netzwerke relevante Informationen, in die Hände böswilliger Akteure fallen könnten. Eine abschließende Bewertung ist aufgrund der fehlenden Gesetzesbegründung und einer europarechtlichen Einordnung derzeit nicht möglich. Zu diesem Aspekt sehen wir im politischen Verfahren weiteren Diskussionsbedarf. In die Beratungen sollten die betroffenen Unternehmen eng eingebunden werden.

IT-Sicherheitskennzeichnung EU-weit einheitlich gestalten

Eine spezielle IT-Sicherheitskennzeichnung kann zu mehr Transparenz über die Sicherheitseigenschaften und zu einer Sensibilisierung auch der kleineren geschäftlichen Anwender für sicherere IT-basierte Produkte beitragen. Dieser Mehrwert ist mit der vorgesehenen nationalen Regelung jedoch nicht gegeben. Die Akzeptanz einer IT-Sicherheitskennzeichnung wird umso höher sein, je besser die Nutzer dessen Aussagegehalt verstehen. Ein IT-Sicherheitskennzeichen wird nur dann einen Mehrwert haben, wenn es europaweit einheitlich ausgestaltet ist.

Bei der Einführung eines freiwilligen IT-Sicherheitskennzeichens sollte darauf geachtet werden, dass die zusätzlichen Belastungen gerade für kleine und mittlere Hersteller möglichst geringgehalten werden. Sinnvoll ist ein abgestuftes Vorgehen je nach erforderlichem Sicherheitsniveau der Produkte. Die Sicherheitsanforderungen der jeweiligen Produktklassen und die Prüftiefe sollten verhältnismäßig sein und gemeinsam mit den betroffenen Unternehmen (insbesondere kleine und mittlere Unternehmen und Startups) auf Basis EU-weiter und internationaler Standards erarbeitet werden. Ein solches Kennzeichen kann nur dann eine Wirkung entfalten, wenn es durch entsprechende Kommunikationsmaßnahmen begleitet wird.

Unterstützungsangeboten für KMU mehr Raum geben

Um auch im Digitalen sicher wirtschaften zu können, benötigen Unternehmen weitere konkrete Unterstützungsangebote, die im vorliegenden Entwurf nicht explizit aufgegriffen werden, z. B.:

- Lotsen- bzw. Anlaufstellen für Fragen zur Prävention und für akute IT-Sicherheitsvorfälle. Dort sollten Unternehmen alle relevanten Informationen erhalten,
- eine stärkere Sensibilisierung und Kompetenzaufbau in Unternehmen durch Kampagnen, Informationsangebote und Vermittlung von IT-Sicherheits-Knowhow von der Schule an,
- Ausbau der Fördermöglichkeiten für KMU-Aktivitäten für mehr IT-Sicherheit.

Sofern das Bundesamt für Sicherheit in der Informationstechnik (BSI) hier Unterstützung leisten kann, sollte dies rechtlich verankert und mit einer entsprechenden Personalausstattung hinterlegt sein.

Umsetzungsfristen angemessen gestalten

Für die technische Implementierung der Vorgaben sind angemessene Übergangsfristen vorzusehen.

Wer wir sind

Unter dem Dach des Deutschen Industrie- und Handelskammertags (DIHK) haben sich die 79 Industrie- und Handelskammern (IHKs) zusammengeschlossen. Unser gemeinsames Ziel: Beste Bedingungen für erfolgreiches Wirtschaften.

Auf Bundes- und Europaebene setzt sich der DIHK für die Interessen der gesamten gewerblichen Wirtschaft gegenüber Politik, Verwaltung und Öffentlichkeit ein.

Denn mehrere Millionen Unternehmen aus Handel, Industrie und Dienstleistung sind gesetzliche Mitglieder einer IHK - vom Kiosk-Besitzer bis zum Dax-Konzern. So sind DIHK und IHKs eine Plattform für die vielfältigen Belange der Unternehmen. Diese bündeln wir in einem verfassten Verfahren auf gesetzlicher Grundlage zu gemeinsamen Positionen der Wirtschaft und tragen so zum wirtschaftspolitischen Meinungsbildungsprozess bei.

Grundlage dieser Stellungnahme sind die dem DIHK bis zur Abgabe der Stellungnahme am 09. Dezember 2020 eingegangenen Äußerungen der IHKs sowie Diskussionen mit Verbänden, Wissenschaftlern und Unternehmen. Diese Stellungnahme basiert auf einem Beschluss des DIHK-Vorstands vom 17. Juni 2020 „Digitale Ökosystem als Fundament für den wirtschaftlichen Erfolg gesamtheitlich gestalten“ und auf den Wirtschaftspolitischen und Europapolitischen Positionen der IHK-Organisation. Sollten dem DIHK noch weitere in dieser Stellungnahme noch nicht berücksichtigte relevante Äußerungen zugehen, wird der DIHK diese Stellungnahme entsprechend ergänzen.

Ansprechpartnerin im DIHK

Dr. Katrin Sobania, sobania.katrin@dihk.de

per E-Mail an:

CI1@bmi.bund.de

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
19(4)750

9. Dezember 2020

Stellungnahme von ARD, ZDF und Deutschlandradio

zum Entwurf eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (Zweites IT-Sicherheitsgesetz – IT-SiG 2.0)

Entwurfsstand 2. Dezember 2020

Sehr geehrte Damen und Herren,

ARD, ZDF und Deutschlandradio nehmen die Möglichkeit zur Stellungnahme im Rahmen des Gesetzgebungsverfahrens zum IT-Sicherheitsgesetz 2.0 gerne wahr.

Allerdings ist eine sorgfältige Prüfung des Gesetzentwurfs innerhalb einer Woche kaum möglich. Wir gehen deshalb davon aus, dass während des weiteren Verfahrens erneut Gelegenheit zu einer Stellungnahme gegeben wird.

Es ist zu begrüßen, dass mit dem Entwurf der Versuch unternommen wird, die IT-Sicherheit in Deutschland zu erhöhen.

Aus Sicht der öffentlich-rechtlichen Rundfunkanstalten muss der Gesetzgeber jedoch darauf achten, dass erweiterte staatliche Befugnisse und Verpflichtungen der verschiedenen Marktteilnehmer die verfassungsrechtlich erforderlichen Grenzen zur Wahrung der Rundfunk- und Pressefreiheit einhalten. Dazu gehört eine entsprechende einfachgesetzliche Ausgestaltung, die den aus Art. 5 GG fließenden und verfassungsgerichtlich manifestierten Vorgaben gerecht wird. Beispielhaft zu nennen sind die bestehenden Durchsuchungs- und Beschlagnahmeverbote und Zeugnisverweigerungsrechte für Journalisten bzw. Medienunternehmen.

Alle staatlichen Eingriffe – zu denen auch die polizeilichen und aufsichtsrechtlichen Befugnisse des BSI und anderer Behörden gehören – müssen zwingend Ausnahmetatbestände für den journalistischen Bereich vorsehen. Zudem ist der Grundsatz der Zuständigkeit der Länder für den Sektor Kultur und Medien, der ebenfalls auf diesen verfassungsrechtlichen Erwägungen beruht, stets zu berücksichtigen. Bundesrechtliche Regelungen dürfen demnach Kompetenzen der Länder nicht außer Acht lassen. Sie dürfen nicht im Widerspruch zu landesgesetzlichen bzw. staatsvertraglichen Regelungen stehen oder bei den Adressaten – sowohl seitens der Administration als auch seitens der Betroffenen – zu Missverständnissen und Auslegungsbedarf führen. Letzteres ist bereits nach dem Grundsatz der Bestimmtheit von gesetzlichen Regelungen auszuschließen.

Angesichts der sehr kurzen Frist zur Stellungnahme wird im Folgenden ausschließlich auf drei Aspekte eingegangen, die den öffentlich-rechtlichen Rundfunk betreffen könnten, selbst wenn dies seitens des BMI vermutlich nicht intendiert ist.

Wir regen an, klarstellend die drei folgenden Änderungen in den Gesetzesentwurf aufzunehmen:

1) § 7d BSIG-E: Die Anordnungskompetenz des BSI sollte konsistent zu § 13 Abs. 7 TMG auf geschäftsmäßig angebotene Telemedien beschränkt bleiben. Außerdem sollte der Gesetzgeber in der Begründung klarstellen, dass der Begriff der „Geschäftsmäßigkeit“ nicht die öffentlich-rechtlichen Telemedienangebote erfasst. Denn eine Aufsicht des BSI über Telemedienangebote der Rundfunkanstalten wäre unzulässig: Zum einen kann die Aufsicht über diese Telemedienangebote nur Gegenstand des Landesrechts sein. Zudem anderen verbietet auch der Grundsatz der Staatsferne des öffentlich-rechtlichen Rundfunks eine Fachaufsicht durch das BSI.

2) § 10 Abs. 5 BSIG-E: Wir schlagen vor klarzustellen, dass als „Unternehmen von erheblicher volkswirtschaftlicher Bedeutung“ nur Wirtschaftsunternehmen in Frage kommen, nicht jedoch öffentlich-rechtliche Rundfunkanstalten.

3) § 15d TMG-E: Für die in dieser Vorschrift vorgesehene Meldepflicht an das BKA sollte eine Ausnahme für Anbieter von journalistisch-redaktionellen Telemedien

aufgenommen werden, die diese Daten in Ausübung ihrer journalistisch-redaktionellen Tätigkeit erlangt haben. Diese Ausnahme sollte sich auch auf technische Dienstleister erstrecken, soweit diese für Anbieter journalistisch-redaktioneller Telemedien tätig werden.

Wir erläutern dies nachfolgend.

I. Vorbemerkung: Zur Rolle des öffentlich-rechtlichen Rundfunks im Bereich der IT-Sicherheit

Wir betrachten die Gewährleistung der IT-Sicherheit für die von uns betriebenen Infrastrukturen bereits jetzt als Teil unserer gesetzlichen Aufgaben. Diese verlangen sowohl die zuverlässige Versorgung der Bevölkerung mit Rundfunk- und Telemedienangeboten (vgl. nur §§ 26 bis 33 MedienStV) als auch den angemessenen Schutz personenbezogener Daten (vgl. nur § 12 MedienStV). Insbesondere gilt dies mit Bezug auf das Redaktionsgeheimnis und die Mitwirkung der Rundfunkanstalten am bundesweiten Katastrophen-Warnsystem MoWaS.

Aus diesem Grund engagieren wir uns im Branchenarbeitskreis Medien des UP KRITIS und werden dieses Engagement auch zukünftig fortsetzen. So wurden beispielsweise unter unserer Beteiligung entsprechende branchenspezifische Sicherheitsempfehlungen erarbeitet und innerhalb des UP KRITIS veröffentlicht.

Die Zusammenarbeit mit dem BSI und weiteren Akteuren im Bereich der Cybersicherheit Deutschlands wird für ARD, ZDF und Deutschlandradio auch weiterhin einen großen Stellenwert haben. Darüber hinaus steht der öffentlich-rechtliche Rundfunk in Deutschland bereits seit Jahren in Fragen der IT-Sicherheit untereinander in einem institutionalisierten Austausch und arbeitet gemeinsam an relevanten Themen sowie Empfehlungen und Standards zum angemessenen Stand der Technik für die Anforderungen der Sendeanstalten.

Der Bundesgesetzgeber hat es bei bisherigen Novellierungen des BSIG und der KRITIS-VO vermieden, den Sektor „Medien und Kultur“ über die Verordnung in das BSIG aufzunehmen, weil er diesen richtigerweise als Ländersache betrachtet. Wir entnehmen dem Entwurf, dass dies auch bei dieser Novellierung nicht geplant ist, regen aber an, dies in den drei hier angesprochenen Punkten klarzustellen. Dies auch, damit in Krisensituationen kein Auslegungs- oder Klärungsbedarf für den Rechtsanwender auf der operativen Ebene entsteht.

II. Im Einzelnen:

1. Zu Anordnungskompetenzen gegenüber Telemediendiensteanbietern § 7d BSIG-E

Wir regen folgende Änderung an:

§ 7d BSIG-E wird wie folgt abgewandelt:

„Das Bundesamt kann in begründeten Einzelfällen zur Abwehr konkreter, erheblicher Gefahren für informationstechnische Systeme einer Vielzahl von Nutzern, die von Telemedienangeboten von Diensteanbietern im Sinne des § 13 Absatz 7 des Telemediengesetzes, welche geschäftsmäßig Telemedien anbieten, ~~§ 2 Satz 1 Nummer 1~~ ausgehen, und die durch ungenügende technische und organisatorische Vorkehrungen ~~im Sinne des § 13 Absatz 7 des Telemediengesetzes~~ dergestalt unzureichend gesichert sind, dass sie keinen hinreichenden Schutz bieten vor

1. unerlaubten Zugriffen auf die für diese Telemedienangebote genutzten technischen Einrichtungen oder

2. Störungen, auch soweit sie durch äußere Angriffe bedingt sind,

gegenüber dem jeweiligen Diensteanbieter ~~im Sinne des § 2 Satz 1 Nummer 1 des Telemediengesetzes~~ anordnen, dass dieser die jeweils zur Herstellung des ordnungs-

gemäßen Zustands seiner Telemedienangebote erforderlichen technischen und organisatorischen Maßnahmen ergreift, um den ordnungsgemäßen Zustand seiner Telemedienangebote herzustellen.

Zusätzlich sollte in § 13 Abs. 7 TMG oder in die Begründung des Regierungsentwurfs folgende Klarstellung aufgenommen werden:

Änderung von § 13 Abs. 7 TMG oder Begründung zu § 7d BSIG-E (S. 64 des Entwurfs):

„Geschäftsmäßig angebotene Telemedien sind nur solche Telemedien, die in der Regel gegen Entgelt angeboten werden. Nicht umfasst sind Anbieter von Telemedien mit journalistisch-redaktionell gestalteten Angeboten."

Begründung:

Diese Änderung würde unter dem Gesichtspunkt der Normenklarheit vermeiden, dass es zu Regelungswidersprüchen kommt. In ihrer aktuellen Entwurfsfassung ist die Vorschrift missverständlich: Sie verleiht dem BSI Anordnungskompetenzen gegenüber allen Telemedienanbietern, d.h. auch nicht-wirtschaftlich ausgerichteten Telemedien, da sie auf § 2 Satz 1 Nr. 1 TMG verweist. Hierzu gehören grundsätzlich auch die Telemedienangebote der öffentlich-rechtlichen Rundfunkanstalten. Diese Anordnungskompetenz soll allerdings laut der Entwurfsbegründung (S. 64) zur Durchsetzung von Sicherheitspflichten nach § 13 Abs. 7 TMG dienen. § 13 Abs. 7 TMG adressiert lediglich Anbieter von *geschäftsmäßig* angebotenen Telemedien. Mit „geschäftsmäßig" sind Telemedienangebote gemeint, die nachhaltig geschäftliche Zwecke verfolgen.[1]

Die Telemedienangebote des öffentlichen Rundfunks, die auf der Basis einer staatsvertraglichen Beauftragung angeboten werden (§§ 30 bis33 MedienStV) und im Wesentli-

[1] *Schmitz,* in: Spindler/Schmitz, TMG. 2. Aufl. 2018, § 13 Rn. 82; BT-Drs. 18/4096, S. 34

chen durch Rundfunkbeiträge finanziert sind, fallen nicht in diese Gruppe. Die Auslegung des Begriffs „geschäftsmäßig“ ist allerdings umstritten,[2] und es finden sich Literaturstimmen, die auch gemeinnützige Angebote unter den Begriff fassen wollen.[3] Der Entwurf, der diese Regelung ausdrücklich auf die Gesetzgebungskompetenz für das Recht der Wirtschaft (Art. 74 Abs. 1 Nr. 11 GG) stützt, sollte deshalb unmissverständlich klarstellen, dass unter „geschäftsmäßig“ angebotenen Telemedien demzufolge auch nur wirtschaftliche Telemedien verstanden werden.

Dies könnte durch einen Zusatz in § 13 Abs. 7 TMG erfolgen, laut dem unter „geschäftsmäßigen“ Telemedien nur solche Telemedien zu verstehen sind, die in der Regel gegen Entgelt angeboten werden.[4] Alternativ sollte dies jedenfalls in der Begründung des Entwurfs klargestellt werden.

Bliebe es bei der derzeitigen Formulierung des § 7d BSIG, so könnte das BSI auch gegenüber Anbietern von solchen Telemedien Anordnungen erlassen, die rundfunkähnlich sind und nicht mit wirtschaftlichen Zielen angeboten werden. Dies ist wohl seitens des BMI nicht beabsichtigt, da die Regelung nur der besseren Durchsetzung der Sicherheitspflichten des § 13 Abs. 7 TMG dienen soll, also der Durchsetzung gegenüber geschäftsmäßigen Telemedien. Die Entwurfsbegründung bezieht sich dabei ausdrücklich auf die Gesetzgebungskompetenz des Bundes für das „Recht der Wirtschaft“ (Entwurfsbegründung S. 64). Dem entspricht konsequenterweise – auch im Interesse der Normenklarheit – den Kreis der Normadressaten auf Wirtschaftsunternehmen einzuschränken.

Eine Befugnis des BSI, gegenüber den öffentlich-rechtlichen Rundfunkanstalten Anordnungen in Bezug auf den Betrieb ihrer Telemedienangebote auszusprechen, wäre jedenfalls nicht zulässig: Zum einen sind die öffentlich-rechtlichen Rundfunkanstalten gemeinnützige Anstalten, die von den jeweiligen Ländern getragen werden.[5] Für diese soll und darf das BSI keine Aufsichtskompetenzen ausüben; dies wäre im Hinblick auf die verfassungsmäßig garantierte Rundfunkfreiheit ein Verstoß gegen das Recht der Selbst-

[2] OVG Magdeburg, Beschluss vom 18.5.2017 – 4 L 103/16
[3] *Spindler,* in: Spindler/Schmitz, 2. Aufl. 2018, TMG § 5 Rn. 8; wohl a.A. *Altenhain*, in: Hoeren/Sieber/Holznagel MMR-HdB, Teil 20 Jugendschutz, Rn. 156.
[4] Die beiden Tatbestandsmerkmale, die in § 5 TMG bislang kumulativ verwendet werden, könnten dabei verschmelzen.
[5] Mit Ausnahme der Deutschen Welle.

verwaltung der Rundfunkanstalten. Darüber hinaus wäre das im Grundgesetz vorgesehene Kompetenzgefüge (Art. 83-85 GG) betroffen. Regelungen zur Aufsicht über die IT-Sicherheit der Anstalten sind mithin Ländersache.

Die Rundfunkanstalten sind, da sie in Erfüllung des Rundfunkauftrags handeln, aus verfassungsrechtlichen Gründen staatsfern organisiert.[6] Der Gesetzgeber ist nach ständiger Rechtsprechung des BVerfG verpflichtet, organisatorischer Maßnahmen zur Sicherung der Rundfunkfreiheit zu treffen und dabei immer den Grundsatz der Staatsferne zu beachten.[7] Die unmittelbare Aufsicht durch staatliche Behörden in rundfunkrechtlichen Angelegenheiten ist deshalb ausgeschlossen oder auf Fragen der Rechtsaufsicht beschränkt.

Eine unmittelbare Aufsichtskompetenz des BSI (als Bundesbehörde) über Telemedienangebote von Landesrundfunkanstalten wäre auch mit dem Aufgabenzuschnitt des BSI nicht vereinbar. Das BSI kann als nationale Cybersicherheitsbehörde den Stellen der Länder Beratung und Unterstützung anbieten (§ 2 Abs. 1 Nr. 13 lit. b, Nr. 13a, Nr. 14, Abs. 2 BSIG). Es hat jedoch – anders als gegenüber dem Bund, § 8 BSIG – gegenüber den Stellen der Länder keine Exekutivkompetenzen. Dies fällt aus den o.g. Gründen in den Bereich der Länder selbst, wobei diese im Rahmen von Kooperationsabkommen auch auf die Unterstützung des BSI zurückgreifen können.

All diese Gründe sprechen dafür, die o. g. Klarstellung vorzunehmen und hierdurch den Adressatenkreis auf nur geschäftsmäßig, d. h. wirtschaftlich angebotene Telemedienangebote zu beschränken und journalistisch-redaktionell gestaltete Angebote vom Anwendungsbereich auszuschließen. Diese Änderung würde die Telemedienangebote des öffentlich-rechtlichen Rundfunks ausklammern.

[6] Zuletzt BVerfGE 136, 9.
[7] Seit dem 1. Rundfunkurteil - BVerfGE 12, 205, 262.

2. Kein „Unternehmen im besonderen öffentlichen Interesse“ im Sinne des BSIG-E

In die Begründung des Regierungsentwurfs sollte folgende Klarstellung aufgenommen werden:

Ergänzung der Begründung zu § 2 Nr. 14 BSIG-E (S. 45 des Entwurfs): „Als Unternehmen von erheblicher volkswirtschaftlicher Bedeutung für die Bundesrepublik Deutschland kommen ausschließlich Wirtschaftsunternehmen in Frage. Die öffentlich-rechtlichen Rundfunkanstalten fallen, auch soweit ihre Tätigkeiten volkswirtschaftliche Bedeutung haben, nicht in diese Kategorie.“

Begründung:

§ 2 Abs. 14 des BSIG-E definiert die neue Kategorie der „Unternehmen im besonderen öffentlichen Interesse“, einschließlich der Untergruppe der Unternehmen mit erheblicher volkswirtschaftlicher Bedeutung (§ 2 Abs. 14 Nr. 2 BSIG-E). Diese werden u. a. in § 8f BSIG-E zusätzlichen IT-Sicherheitspflichten unterworfen. Die wirtschaftlichen Kennzahlen, nach denen sich die Unternehmen mit dieser besonderen volkswirtschaftlichen Bedeutung bestimmen sollen, werden in einer Rechtsverordnung des BMI festgelegt, die auf Basis von § 10 Abs. 5 BSIG ergeht.

In der Begründung heißt es hierzu auf S. 44, dass die Berechnungsmethodik der „volkswirtschaftlichen Bedeutung“ und auch die erfassten Unternehmen sich an dem Gutachten der Monopolkommission nach § 44 Absatz 1 GWB (sog. Hauptgutachten) orientieren sollen. In den bisherigen Gutachten der Monopolkommission sind öffentlich-rechtliche Rundfunkanstalten nicht erwähnt.

Wir gehen deshalb davon aus, dass die Kategorie der „Unternehmen mit erheblicher volkswirtschaftlicher Bedeutung“ nicht die öffentlich-rechtlich organisierten Rundfunkanstalten erfassen soll, regen aber an, dies klarstellend im Gesetz zu regeln. Dies sollte

auf der Ebene der Verordnungsermächtigung, jedenfalls aber in der gesetzlichen Begründung klargestellt werden. Eine genauere Festlegung der Kriterien der „volkswirtschaftlichen Bedeutung“ würde auch die Rechtssicherheit der Verordnung vor dem Hintergrund von Art. 80 Abs. 1 Satz 2 GG erhöhen.

Eine Behandlung von öffentlich-rechtlichen Rundfunkanstalten als „Unternehmen von besonderem öffentlichem Interesse“ wäre auch nicht sachgerecht: Die öffentlich-rechtlichen Rundfunkanstalten sind aus den oben genannten Gründen aufgrund ihrer staatsfernen Organisation und ihrer gesetzgeberischen „Zugehörigkeit“ zu den Ländern einer Aufsicht durch das BSI und einer sektorspezifischen Regulierung durch Bundesrecht nicht zugänglich. Dies folgt aus der Rundfunkfreiheit, aus der fehlenden Verwaltungskompetenz des Bundes (für die Aufsicht durch das BSI über Landesrundfunkanstalten) und der fehlenden Gesetzgebungskompetenz des Bundes. Die als Grundlage für die meisten Novellierungen des BSIG herangezogene Kompetenz des Art. 74 Abs. 1 Nr. 11 GG („Recht der Wirtschaft“) lässt sich nicht als Grundlage für Rechtspflichten heranziehen, die die öffentlich-rechtlichen Rundfunkanstalten auch im Bereich ihrer Auftragserfüllung betreffen würden.

3. Zu Meldepflichten der Rundfunkanstalten als Telemedienanbieter § 15d TMG-E

Wir regen folgende Änderung an:

Unter § 15d TMG-E wird folgender Absatz 3 ergänzt: „Die vorstehenden Pflichten betreffen nicht Anbieter von Telemedien mit journalistisch-redaktionell gestalteten Angeboten, die diese Daten in Ausübung ihrer journalistisch-redaktionellen Tätigkeit erlangt haben. Gleiches gilt für technische Dienstleister, soweit diese für Anbieter von Telemedien mit journalistisch-redaktionell gestalteten Angeboten tätig werden.“

Begründung:

Nach § 15d TMG-E sollen alle Anbieter von Telemedien, und somit auch die öffentlich-rechtlichen Rundfunkanstalten, verpflichtet sein, im Fall einer „unrechtmäßigen Übermittlung oder unrechtmäßigen Kenntniserlangung von Daten“, die eventuell durch Straftaten nach § 202a-202d StGB erlangt wurden, das BKA in Kenntnis zu setzen. Voraussetzung hierfür ist außerdem, dass von den Daten eine gewisse Gefährlichkeit ausgeht, beispielsweise für eine große Zahl von Personen oder den Datenbestand von Bundesbehörden.

Ausweislich der Begründung des Entwurfs greift diese Informationspflicht sowohl dann, wenn die Daten über den Telemediendiensteanbieter übermittelt werden, als auch wenn er selbst oder Dritte von den Daten über sein Angebot Kenntnis erhalten (Begründung S. 89 und 90).

Würde diese Berichtspflicht auch für die Telemedienangebote der öffentlich-rechtlichen Rundfunkanstalten greifen, würde dies auch ihre Aufgabenerfüllung betreffen. Würden Dritte oder die Rundfunkanstalten selbst im Rahmen ihrer Angebote solche Daten offen legen, müssten sie das BKA über sämtliche Informationen unterrichten, „die für die Beurteilung des jeweiligen Einzelfalls und davon abhängigen Folgemaßnahmen der jeweils zuständigen Behörden auf dem Gebiet der Strafverfolgung und Gefahrenabwehr maßgeblich sind“ (Begründung S. 90). Die Rundfunkanstalten hätten also sehr umfangreiche Informationspflichten gegenüber dem BKA.

Eine derartige Melde- und Informationspflicht der Rundfunkanstalten ist jedoch mit deren verfassungsrechtlichen Aufgabe nicht vereinbar. Das Angebot von Telemedien durch die Rundfunkanstalten gehört unmittelbar zu deren Rundfunkauftrag (vgl. nur §§ 30-33 MedienStV) und ist deshalb staatsfern zu organisieren.[8]

Insbesondere schützt die Rundfunkfreiheit auch die Entgegennahme und Veröffentlichung von Daten gezielt zur Gewinnung von journalistisch relevanten Erkenntnissen. Dies kann gerade die Einsendung oder Veröffentlichung von rechtswidrig erlangten Daten über Telemedienangebote betreffen. Als hypothetisches Beispiel sei genannt, dass

[8] Programmautonomie; vgl. nur BVerfGE 90, 60, 92 ff.; 59, 231, 258.

ein Nutzer auf ein öffentlich-rechtliches Telemedienangebot ein „geleaktes“ Dokument hoch lädt, das eine Korruptionsaffäre aufdeckt. Nutzer, die in solchen Fällen Informationen beitragen, haben in solchen Fällen denselben Status wie journalistische Quellen. Das Recht von Medienanbietern, deren Anonymität zu schützen, hat Verfassungsrang.[9] Die Gewährleistung umfassenden Informanten- und Quellenschutzes sowie der Schutz journalistisch redaktioneller Inhalte betreffen den Kernbereich der Rundfunkfreiheit. Dies gilt gerade auch dann, wenn die Informationen auf rechtswidrigem Weg erlangt worden sind (BVerfGE 66, 116 - *Springer/Wallraff*; BVerfGE 20, 162 - *Spiegel*).

Zum Angebot von Telemedien gehört auch deren „Rückkanalfähigkeit“, also die Möglichkeit für Nutzer, eigene Inhalte und Informationen hochzuladen, beispielsweise in Form von Nutzerkommentaren oder Videos. Wenn die Rundfunkanstalten den Nutzern dies im Rahmen ihrer Telemedien ermöglichen, unterfällt auch dies dem Schutzbereich der Rundfunkfreiheit.[10]

Es ist deshalb ein essenzielles Interesse der Rundfunkanstalten, journalistischen Quellenschutz ggf. auch denjenigen Personen gewähren zu können, die öffentlich-rechtliche Telemedienangebote nutzen, um dort evtl. rechtswidrig erlangte Informationen zu veröffentlichen oder an die Rundfunkanstalten zu übermitteln. Gleiches gilt, wenn die Rundfunkanstalten selbst solche Informationen im Rahmen ihrer Telemedienangebote veröffentlichen.

Selbstverständlich würden die Rundfunkanstalten im Fall von typischer, rein wirtschaftlich oder terroristisch motivierter Cyberkriminalität mit den zuständigen Behörden zusammenarbeiten. Im Fall von Informationen, die für die öffentliche Meinungsbildung von hoher Relevanz sind, muss es ihnen aber überlassen bleiben, die Anonymität der Personen, die diese Daten zur Verfügung gestellt haben, ggf. vor staatlichem Zugriff schützen zu können. Falls öffentlich-rechtliche Rundfunkanstalten im Rahmen ihrer Telemedienangebote an Daten gelangen, die möglicherweise im Rahmen einer Straftat erlangt worden sind, muss die Entscheidung, ob sie Erkenntnisse hierüber an Strafverfolgungsbehörden weitergeben, deshalb ihnen selbst überlassen bleiben. Andernfalls

[9] Statt vieler BVerfGE 77, 65, 75; EGMR v. 11.07.2002 - 28957/95.

würde der verfassungsrechtlich nach Art. 5 Abs.1 Satz 1 GG gebotene und *de lege lata* bestehende umfangreiche Informanten- und Quellenschutz unterlaufen.

Mit freundlichen Grüßen

Bernd Radeck

Justitiar des SR

Peter Weber

Justitiar des ZDF

Dr. Markus Höppener

Justiziar des Deutschlandradio

Deutscher Bundestag

Ausschuss für Inneres und Heimat

Ausschussdrucksache
19(4)751

DIE FAMILIEN UNTERNEHMER

DIE FAMILIENUNTERNEHMER | Charlottenstraße 24 | 10117 Berlin

An die Mitglieder des Innenausschusses
des Deutschen Bundestages
(CDU/CSU, SPD, Bündnis 90/Die Grünen, FDP)
Platz der Republik 1
11011 Berlin

→ Übermittlung per E-Mail

Berlin,
26. Februar 2021

Nachbesserung des IT-Sicherheitsgesetzes 2.0
Stellungnahme von DIE FAMILIENUNTERNEHMER

Sehr geehrte Damen und Herren,

Sie sind im Begriff, mit dem „zweiten Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme“ wesentliche Weichenstellungen für die Sicherheit und Vertrauenswürdigkeit unserer 5G-Mobilfunkinfrastruktur vorzunehmen. Mit diesem Schreiben übermitteln wir die Stellungnahme von DIE FAMILIENUNTERNEHMER dazu.

Das 5G-Netz wird das Zentralnervensystem unseres auf Wissen gestützten Hochtechnologie-Standortes sein. Unternehmen und Bürger müssen sich auf ein sicheres 5G-Netz ohne Spionage- und Sabotagehintertüren verlassen können. Nur so kann die internationale Wettbewerbsfähigkeit unserer Wirtschaft erhalten und damit die Zukunftsfähigkeit unseres Landes gesichert werden. Unternehmen und Bürger vertrauen aus diesem Grund auf ein Sicherheitsgesetz, das diesen Schutz verlässlich leistet.

In seiner derzeitigen Form ist das nicht gegeben. Der Gesetzentwurf leidet im Gegenteil an einem fundamentalen Konstruktionsfehler, indem gemäß § 9b Komponenten zweifelhafter Anbieter automatisch verbaut werden dürfen, solange nicht alle beteiligten Ministerien geschlossen für einen Ausschluss dieses Anbieters stimmen.

Mögliche Sicherheitsbedenken nur eines Ressorts - und seien sie auch noch so begründet! - würden nicht ausreichen. Mit derartigen hohen Verbotshürden würde faktisch der gesamte Prüfprozess entwertet. DIE FAMILIENUNTERNEHMER appellieren daher an Sie, diese Regelung zu verbessern.

Albrecht von der Hagen
Hauptgeschäftsführer und
Mitglied des Bundesvorstands
Charlottenstraße 24
10117 Berlin

Tel. 030 300 65-310
Fax 030 300 65-390

vdhagen@familienunternehmer.eu

Es sollte stattdessen entweder das Parlament bei der Überprüfung der politischen Vertrauenswürdigkeit beteiligt oder hilfsweise ein Genehmigungsvorbehalt vorgesehen werden. Entscheidend aber ist, nur solche Hersteller für den 5-G-Netzausbau zuzulassen, gegen die keine Sicherheitsbedenken erhoben werden.

Denn nur eine sichere Technologie bietet die Gewähr, im Zuge der Transformation zur Industrie 4.0, dem „Internet der Dinge“ und der Nutzung künstlicher Intelligenz nicht ins Hintertreffen zu geraten oder uns gar abhängig zu machen, sondern verloren gegangenes Terrain zurückzugewinnen. Bitte sorgen Sie mit dafür, dass wir beim Zukunftsthema 5G auf diese Weise unsere beiden verbliebenen europäischen Anbieter von 5G-Komponenten unterstützen.

Mit freundlichen Grüßen

[redacted]

Albrecht von der Hagen
Hauptgeschäftsführer und Mitglied des Bundesvorstands

Anlage

STELLUNGNAHME

DIE FAMILIEN UNTERNEHMER

DIE JUNGEN UNTERNEHMER

Letzter Weckruf für die Sicherheit

Entwurf eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0)

Angesichts zunehmender Cyberattacken auf Krankenhäuser, Behörden und Mittelständler rückt die Frage der Datensicherheit und der digitalen Souveränität immer mehr in das Bewusstsein. Beim Schutz der betrieblichen IT gewinnt auch die Abwehr von Wirtschaftsspionage und Sabotage an Bedeutung: Denn mit relativ geringen Aufwand könnten sensible Geschäftsgeheimnisse abgefischt und sogar zentrale Infrastrukturen wie die Daseinsvorsorge aus der Ferne abgeschaltet werden.

Mit dem derzeit laufenden Aufbau der 5G-Mobilfunkinfrastruktur wird das Fundament für die Zukunftsfähigkeit Deutschlands gelegt. Gerade im Zuge der Transformation zur Industrie 4.0, dem „Internet der Dinge“ und der Nutzung künstlicher Intelligenz kommt dem künftigen 5G-Netzen große Bedeutung zu. Das 5G-Netz wird das Zentralnervensystem unseres auf Wissen gestützten Hochtechnologie-Standortes. Unternehmen und Bürger müssen sich aus diesem Grund auf ein sicheres 5G-Netz ohne Spionage- und Sabotagehintertüren verlassen können. Nur auf diese Weise kann auch der Wunsch nach digitaler Souveränität erreicht werden.

Unsicherheitsgesetz? Kompromisse bei der Sicherheit

Deshalb muss der Sicherheit kritischer Infrastrukturen besondere Aufmerksamkeit geschenkt werden. Mit dem „zweiten Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme“ (kurz IT-Sicherheitsgesetz 2.0) hat die Bundesregierung kurz vor Weihnachten dazu einen Entwurf vorgelegt.

Neben der Erfüllung technischer Sicherheitskriterien soll laut Gesetzesentwurf auch die politische Vertrauenswürdigkeit der Hersteller von Ausrüstung für das 5G-Netz geprüft werden: Nimmt ein fremder Staat Einfluss auf das Privatunternehmen? Handelt es sich beim Herkunftsland des Herstellers um eine Demokratie mit rechtsstaatlichen Strukturen? Gibt es dort Regelungen, die das Unternehmen zur Datenherausgabe an das Regime verpflichtet?

Was erst einmal gut klingt, entpuppt sich in der Gesetzesausgestaltung allerdings als Mogelpackung. Zwar ist es positiv, dass mit dem Gesetz versucht wird die Cybersicherheit zu stärken, aber in Bezug auf den vertrauenswürdigen 5G-Netzaufbau handelt es sich um ein „Unsicherheitsgesetz“. Anstatt die Chance zu nutzen, Deutschland wirklich sicher und damit zukunftsfähig zu machen, ist das Design der Entscheidungsprozesse über die Frage, ob ein

DIE FAMILIENUNTERNEHMER e.V.
DIE JUNGEN UNTERNEHMER
Dr. Julian Dörr
Charlottenstraße 24 | 10117 Berlin

Tel. 030 300 65-443
Fax 030 300 65-390
doerr@familienunternehmer.eu
www.familienunternehmer.eu

Stand: 26. Februar 2021

Anbieter „vertrauenswürdig“ ist, so angelegt, dass es in der Praxis kaum je final zu einem Ausschuss kommen werden dürfte.

Denn leider ist für den Prüfprozess lediglich der so genannte Untersagungsvorbehalt vorgesehen: Sollten nicht alle beteiligten Ministerien geschlossen für einen Ausschluss zweifelhafter Hardware stimmen, darf sie automatisch verbaut werden. Mögliche Sicherheitsbedenken nur eines Ressorts würden nicht ausreichen. Aufgrund solcher hohen Verbotshürden würden faktisch alle Komponenten durchgewinkt und der gesamte Prüfprozess entwertet. Damit öffnen wir das 5G-Netz bereitwillig Anbieter aus Staatswirtschaften und Diktaturen, die auch mit staatlich verschleierten Dumpingpreisen versuchen Marktmacht zu gewinnen.

Vernünftiger wäre es aus Sicht deutscher Hochtechnologie-Anbieter, wenn die Entscheidung über die politische Vertrauenswürdigkeit der Anbieter von 5G-Komponenten einem Gremium des Bundestages übertragen werden würde. Hilfsweise sollte im IT-Sicherheitsgesetz zumindest die aktive Zustimmung aller beteiligter Ministerien festgeschrieben werden (Genehmigungsvorbehalt): Nur falls sämtliche Beteiligte keine Sicherheitsbedenken haben, sollten Hersteller für den 5G-Netzausbau zugelassen werden.

Deutschland würde mit dem derzeit vorliegenden Entwurf eines Sicherheitsgesetzes einen Sonderweg gehen und sich in Europa isolieren. Vorbilder sollten uns Großbritannien, Frankreich und Schweden sein, die die potentielle Einflussnahme durch einen fremden Staat nicht akzeptieren und durch strikte Prüfungen sichere 5G-Netze aufbauen.

DIE FAMILIENUNTERNEHMER haben wiederholt deutlich gemacht, dass für uns auf Dauer angelegte, nachhaltige Datensouveränität schwerer wiegt als mögliche Benachteiligungen für deutsche Akteure auf z. B. asiatischen Teilmärkten, falls die politische Führung von nicht-europäischen Anbietern deutsche Unternehmen im Kontext einer 5G-Regulierung abstrafen sollte. Datensicherheit, Schutz vor Manipulation sowie Erpressbarkeit und technologische Unabhängigkeit sind gerade für unsere deutschen Technologie-Champions überlebenswichtig.

Nachbesserungen und Änderungen im Einzelnen

- Sämtliche nachfolgende Änderungsvorschläge beziehen sich auf Absätze des § 9b „Untersagung des Einsatzes kritischer Komponenten“ des IT-Sicherheitsgesetz-Entwurfes (aufgeführt unter dem Abschnitt „19. Nach §9 werden die folgenden §§ 9a bis 9c eingefügt“).

- 5G-Netze sind in ihrer Gesamtheit kritische Infrastrukturen und als solche insgesamt zu prüfen, eine Differenzierung des Vorbehaltes einer Vertrauenswürdigkeitsprüfung anhand einer anderweitig geregelten Zertifizierungspflicht ist nicht sinnvoll. Entsprechender Nebensatz sollte gestrichen werden:

DIE FAMILIENUNTERNEHMER e.V.
DIE JUNGEN UNTERNEHMER
Dr. Julian Dörr
Charlottenstraße 24 | 10117 Berlin

Tel. 030 300 65-443
Fax 030 300 65-390
doerr@familienunternehmer.eu
www.familienunternehmer.eu

§ 9b Absatz 1

(1) Der Einsatz kritischer Komponenten gemäß § 2 Absatz 13~~, für die eine gesetzliche Zertifizierungspflicht besteht,~~ ist durch den Betreiber der Kritischen Infrastruktur dem Bundesministerium des Innern, für Bau und Heimat vor Einsatz anzuzeigen. In der Anzeige ist die kritische Komponente und die Art ihres Einsatzes anzugeben. ~~Die Pflicht aus Satz 1 besteht bereits dann, wenn für die Pflicht zur Vorlage von Zertifikaten eine Übergangsfrist gewährt wird.~~

- Die Selbsterklärung (Garantieerklärung) eines Herstellers ist keine hinreichende Bedingung für die Vertrauenswürdigkeit des jeweiligen Herstellers. Stattdessen sollte vielmehr durch die beteiligten Ressorts eine grundlegende Überprüfung der Vertrauenswürdigkeit im Sinne einer Bewertung des Risikoprofils von Herstellern erfolgen. Entsprechend sollte § 9b (2) umformuliert werden:

§ 9b Absatz 2

(2) Kritische Komponenten gemäß § 2 Absatz 13 dürfen nur eingesetzt werden, wenn **das Bundesministerium des Innern, für Bau und Heimat im Einvernehmen mit dem Auswärtigen Amt, dem Bundeskanzleramt und dem Bundesministerium der Verteidigung** ~~der Hersteller eine Erklärung über seine~~ **die Vertrauenswürdigkeit** ~~gegenüber dem Betreiber der Kritischen Infrastruktur (Garantieerklärung) abgeben~~ **des Herstellers der kritischen Komponenten festgestellt hat.**

~~Diese Erklärung erstreckt sich auf die gesamte Lieferkette des Herstellers. Die Garantieerklärung des Herstellers der kritischen Komponente ist der Anzeige nach Absatz 1 beizufügen. Aus der Garantieerklärung muss unter anderem hervorgehen, ob und wie der Hersteller hinreichend sicherstellen kann, dass die kritische Komponente über keine technischen Eigenschaften verfügt, die geeignet sind, missbräuchlich, insbesondere zum Zwecke von Sabotage, Spionage oder Terrorismus auf die Sicherheit, Integrität, Verfügbarkeit oder Funktionsfähigkeit der Kritischen Infrastruktur einwirken zu können. Das Bundesministerium des Innern, für Bau und Heimat legt die Mindestanforderungen für die Garantieerklärung im Einvernehmen mit den betroffenen Ressorts unter Berücksichtigung überwiegender öffentlicher Interessen, insbesondere sicherheitspolitischer Belange, durch Allgemeinverfügung fest, die im Bundesanzeiger bekannt zu machen ist. Das Verbot in Satz 1 gilt erst ab der Bekanntmachung der Allgemeinverfügung nach Satz 5. Soweit Änderungen der Allgemeinverfügung erfolgen, sind diese für bereits nach Absatz 2 abgegebene Garantieerklärungen unbeachtlich.~~

- Entsprechend der eingangs ausgeführten Ablehnung lediglich eines Untersagungsvorbehaltes sollte stattdessen ein Genehmigungsvorbehalt verankert werden:

§ 9b Absatz 3, 4

(3) Das Bundesministerium des Innern, für Bau und Heimat ~~kann~~ **muss** den Einsatz ~~einer~~ **aller** kritischen Komponenten **eines Herstellers** gegenüber dem Betreiber der Kritischen Infrastruktur im Einvernehmen mit ~~den betroffenen Ressorts~~ **dem Auswärtigen Amt, dem Bundeskanzleramt und dem Bundesministerium der Verteidigung** bis zum Ablauf von ~~einem Monat~~ **drei Monaten** nach Eingang der Anzeige nach Absatz 1 ~~untersagen~~ **erlauben** oder Anordnungen erlassen, wenn überwiegende öffentliche Interessen, insbesondere sicherheitspolitische Belange der Bundesrepublik Deutschland **oder mangelnde Vertrauenswürdigkeit des Herstellers**, dem Einsatz entgegenstehen. Vor Ablauf der Frist von ~~einem~~ **drei** Monaten **nach** Anzeige nach Absatz 1 ist der Einsatz nicht gestattet.

(4) Das Bundesministerium des Innern, für Bau und Heimat **muss** ~~kann~~ den weiteren Betrieb **aller kritischen Komponenten eines Herstellers** ~~einer kritischen Komponente gegenüber dem Betreiber der Kritischen Infrastruktur~~ im Einvernehmen **mit dem Auswärtigen Amt, dem Bundeskanzleramt und dem Bundesministerium der Verteidigung** ~~den betroffenen Ressorts~~ **untersagen** ~~oder Anordnungen erlassen~~, wenn der Hersteller der kritischen Komponente sich als nicht vertrauenswürdig erwiesen hat.

- Vertrauenswürdigkeit kann nicht durch technische Kriterien überprüft werden, da sie nicht-technische Risiken ausklammert. Entsprechend sollte das Gesetz bei der Definition der Vertrauenswürdigkeit eines Herstellers weder allein technische Kriterien heranziehen noch die strategischen, nicht-technischen Kriterien in nachgelagerte Verordnungen verschieben.

§ 9b Absatz 5

(5) Ein Hersteller einer kritischen Komponente ist nicht vertrauenswürdig, wenn
~~1. er gegen die in der Garantieerklärung eingegangen Verpflichtungen und Versicherungen verstoßen hat,~~
~~2. die in der Garantieerklärung angegebenen Tatsachen unwahr sind,~~
~~3. er Sicherheitsüberprüfungen und Penetrationsanalysen nicht im erforderlichen Umfang an seinem Produkt und in der Produktionsumgebung in angemessener Weise unterstützt,~~
~~4. er bekannte oder bekannt gewordene Schwachstellen oder Manipulationen nicht unverzüglich dem Betreiber der Kritischen Infrastruktur meldet und beseitigt oder~~
~~5. die kritische Komponente über technische Eigenschaften verfügt oder verfügt hat, die geeignet sind oder waren, missbräuchlich auf die Sicherheit, Integrität, Verfügbarkeit oder Funktionsfähigkeit der Kritischen Infrastruktur einwirken zu können. Ein Verstoß nach Nummer 5 liegt nicht vor, wenn der Hersteller nachweisen kann, dass er die technische Eigenschaft im Sinne von Nummer 5 nicht implementiert hat und er diese jeweils ordnungsgemäß beseitigt hat.~~

1. eine hohe Wahrscheinlichkeit einer Einwirkung von Regierungsorganisationen eines Drittstaates auf den Hersteller besteht.

2. die Möglichkeit der Einflussnahme auf den Hersteller durch gesetzgeberische Akte eines Drittstaates besteht, falls der Hersteller in diesem Drittstaat seinen Sitz hat.

3. Sicherheits- oder Datenschutzübereinkommen zwischen der Europäischen Union und dem Sitzstaat des Lieferanten fehlen, sofern es sich dabei um einen Drittstaat handelt.

4. die Fähigkeit eines Drittstaates, Druck auf den Hersteller auszuüben, vorhanden ist, insbesondere hinsichtlich des Produktionsstandorts.

5. bestimmte Charakteristika in der Eigentümerstruktur des Herstellers vorhanden sind, die eine Einflussnahme eines Drittstaates ermöglichen.

- Die Konsequenz eines Ausschlusses nicht-vertrauenswürdiger Hersteller greift nicht weit genug, da sie lediglich auf die Untersagung des Einsatzes einzelner Komponenten abstellt und damit rein technischen Erwägungen folgt. Deutschland sollte sich an der EU 5G Toolbox (Cybersecurity of 5G networks – EU Toolbox of risk mitigating measures) orientieren: Länder wie Großbritannien (de jure) und Frankreich (de facto) verfahren nach einem Phase-Out-Modus für bereits verbaute Komponenten nicht-vertrauenswürdiger Hersteller.

§ 9b Absatz 6, 7

~~(6) Wurde nach Absatz 4 der Einsatz einer kritischen Komponente untersagt, kann das Bundesministerium des Innern, für Bau und Heimat im Einvernehmen mit den betroffenen Ressorts~~
~~1. den angezeigten Einsatz weiterer kritischer Komponenten desselben Typs und desselben Herstellers untersagen und~~
~~2. nach Ablauf einer angemessenen Frist die Nutzung bereits im Einsatz befindlicher kritischer Komponenten desselben Typs und desselben Herstellers untersagen.~~

~~(7) Bei wiederholter Feststellung nicht vorliegender Vertrauenswürdigkeit nach Absatz 5 Nummer 1 bis 3 kann das Bundesministerium des Innern, für Bau und Heimat im Einvernehmen mit den betroffenen Ressorts den Einsatz aller kritischen Komponenten des Herstellers untersagen.~~

(6) Bereits verbaute Komponenten eines Herstellers, der sich im Nachhinein als nicht-vertrauenswürdig erwiesen hat, dürfen nach einer Frist von 5 Jahren nach Inkrafttreten dieses Gesetzes nicht mehr eingesetzt werden.

DIE FAMILIENUNTERNEHMER e.V.
DIE JUNGEN UNTERNEHMER
Dr. Julian Dörr
Charlottenstraße 24 | 10117 Berlin

Tel. 030 300 65-443
Fax 030 300 65-390
doerr@familienunternehmer.eu
www.familienunternehmer.eu

Berlin, 18. Januar 2021

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
19(4)753

bdew
Energie. Wasser. Leben.

BDEW Bundesverband der Energie- und Wasserwirtschaft e. V.
Reinhardtstraße 32
10117 Berlin

www.bdew.de

Fakten und Argumente

zu einem „Zweiten Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme“ (IT-SiG 2.0)

Der Bundesverband der Energie- und Wasserwirtschaft (BDEW), Berlin, und seine Landesorganisationen vertreten über 1.900 Unternehmen. Das Spektrum der Mitglieder reicht von lokalen und kommunalen über regionale bis hin zu überregionalen Unternehmen. Sie repräsentieren rund 90 Prozent des Strom- und gut 60 Prozent des Nah- und Fernwärmeabsatzes, 90 Prozent des Erdgasabsatzes, über 90 Prozent der Energienetze sowie 80 Prozent der Trinkwasser-Förderung und rund ein Drittel der Abwasser-Entsorgung in Deutschland.

Überblick

Der Bundesverband der Energie- und Wasserwirtschaft (BDEW) vertritt über 1900 Unternehmen. Das Spektrum der Mitglieder reicht von lokalen und kommunalen über regionale bis hin zu überregionalen Unternehmen. Sie repräsentieren rund 90 Prozent des Stromabsatzes, gut 60 Prozent des Nah- und Fernwärmeabsatzes, 90 Prozent des Erdgasabsatzes sowie 80 Prozent der Trinkwasser-Förderung und rund ein Drittel der Abwasser-Entsorgung in Deutschland. Außerdem vereint der BDEW 94 Prozent der Stromnetzlänge, 92 Prozent der Gasnetzlänge und 78 Prozent der Wärme- bzw. Kältenetzlänge.

Das Bundeskabinett hat am 16. Dezember 2020 auf Vorlage des Bundesministeriums des Innern, für Bau und Heimat einen Entwurf verabschiedet eines „Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme“, kurz IT-Sicherheitsgesetz 2.0 (IT-SiG 2.0). An den Kabinettsbeschluss schließt sich das parlamentarische Verfahren an.

Grundsätzlich begrüßt der BDEW die Überarbeitung und Weiterentwicklung des Ordnungsrahmens zum Schutz Kritischer Infrastrukturen durch die Bundesregierung. Sichere informationstechnische Systeme sind für die Aufrechterhaltung der Energie- und Wasserver- bzw. -entsorgung von zentraler Bedeutung. Angesichts der dynamischen Entwicklung der Bedrohungen aus dem digitalen Raum stehen wir zu dem Ziel, die Informationssicherheit der Energie- und Wasserversorgung zu erhöhen. Auf Grundlage des vorliegenden Gesetzesentwurfs sind jedoch massive wirtschaftliche Auswirkungen auf die Betreiber Kritischer Infrastrukturen zu erwarten, die dringend adressiert werden sollten, insbesondere die Pflichten zur Einholung einer Garantieerklärung für „kritische Komponenten“, zum Einsatz von Systemen zur Angriffserkennung, die drastische Verschärfung von Bußgeldern und die Gefahr der Doppelregulierung großer Unternehmen.

Einschätzung

Wir begrüßen ausdrücklich, dass Hersteller und Anbieter von IT-Produkten nach § 7a zukünftig einen größeren Beitrag zum Schutz von Kritischen Infrastrukturen leisten sollen. Nur durch eine vertrauensvolle und enge Kooperation zwischen Herstellern und Betreibern kann die IT-Sicherheit von in der Energie- und Wasserwirtschaft eingesetzten Komponenten, Dienstleistungen und Prozessen effizient erhöht und entstehende Sicherheitsrisiken vermindert werden. Insofern stellt diese vorgeschlagene Neuerung einen erheblichen Schritt nach vorne dar.

Es ist jedoch abzusehen, dass erwogene Neuregelungen des Gesetzentwurfs zum Teil erhebliche negative Auswirkungen auf die Betreiber Kritischer Infrastrukturen haben werden. Insbesondere folgende Aspekte gilt es aus Sicht des BDEW dringend zu überdenken:

1. Garantieerklärung nach § 2 Abs. 13 BSIG-E i. V. m. § 9b BSIG-E

In § 2 Abs. 13 soll der Begriff der „kritischen Komponenten“ bestimmt werden. Dieser Begriff und die sich daraus ableitende Gesetzgebung bezieht sich bisher ausschließlich auf den Sektor Telekommunikation. In § 9b wird wiederum die Pflicht zur Einholung einer Garantieerklärung für „kritische Komponenten“ eingeführt. Demnach sollen Betreiber Kritischer Infrastrukturen in Sektoren, in denen eine Zertifizierungspflicht für „kritische Komponenten“ besteht, nur

noch von denjenigen Herstellern IT-Produkte einsetzen dürfen, von denen eine Garantieerklärung über die Vertrauenswürdigkeit ihrer Produkte vorliegt. In der jetzigen Form soll dies bisher ausschließlich den Telekommunikationssektor treffen. Mit der vorgeschlagenen Neuregelung soll allerdings eine gesetzliche Grundlage geschaffen werden, die eine spätere Ausweitung auf weitere Sektoren, wie die Energie- und Wasserwirtschaft ermöglicht.

Die Einführung einer solchen Zertifizierungspflicht in bestehenden Infrastrukturen im energie- und wasserwirtschaftlichen Umfeld ist eine hochsensible Angelegenheit. Die Auswirkungen sind in dem komplexen Einsatzumfeld vielfältig. Beispielsweise könnte eine ausbleibende (Re-)Zertifizierung eines Herstellers dazu führen, dass Komponenten dieses Herstellers von Betreibern Kritischer Infrastrukturen nicht weiterverwendet werden dürfen, also vollständig ausgetauscht werden müssen. Die Kosten hierfür müssten die Betreiber tragen, obwohl ein sicherer Komponenteneinsatz weiterhin möglich wäre. Weiterhin ist von einer Preiserhöhung von kritischen Komponenten auszugehen, da voraussichtlich weniger Anbieter am Markt zur Verfügung stehen werden und diese die Kosten der Zertifizierung auf ihre Kunden umlegen. Unter dem Strich würde eine solche Zertifizierungspflicht von „kritischen Komponenten“ in Verbindung mit der Einholung einer Garantieerklärung einen fragwürdigen Nutzen für die Informationssicherheit der Energie- und Wasserver- und -entsorgung mit sich bringen, da enorme bürokratische Aufwände sowie wirtschaftliche Risiken dem erhofften und vermeintlichen Zugewinn an Vertrauen in die Integrität von IT-Produkten gegenüber stehen.

Die Definition von „kritischen Komponenten“ nach § 2 Absatz 13 kann in der vorliegenden Formulierung deshalb einzig in Telekommunikationsnetzen Anwendung finden. *Die Möglichkeit der Einführung einer Zertifizierungspflicht in weiteren Sektoren sollte dringend aus dem Gesetz gestrichen werden.*

2. Systeme zur Angriffserkennung nach § 8a Abs. 1a BSIG-E und § 11 Abs. 1d EnWG

Mit der Einführung von § 8a Abs 1a sollen Betreiber Kritischer Infrastrukturen verpflichtet werden, sogenannte Systeme zur Angriffserkennung einzuführen und deren Einsatz alle zwei Jahre gegenüber den Aufsichtsbehörden nachzuweisen.

Eine Einführung von Systemen zur Angriffserkennung in prozess- und leittechnischen Einrichtungen ist gegenwärtig nach allgemeinem Stand der Technik kaum bis äußerst aufwändig umsetzbar. Es ist weiterhin nicht wahrscheinlich, dass durch die Einführung der angestrebte Sicherheitszugewinn erreicht wird, da sich derlei Systeme in einem unreifen Entwicklungsstand befinden. Es ist nicht nachvollziehbar, wie z.B. Systeme zur Angriffserkennung eingetretene Störungen beseitigen können, ohne den sicheren Betrieb einer Anlage und damit die Versorgungssicherheit empfindlich zu gefährden. Es muss also festgehalten werden, dass der tatsächliche Nutzen dieser Maßnahme in keinem Verhältnis zum Aufwand ihrer Umsetzung steht. Ebenso sollte von einer Spezifizierung von technischen Maßnahmen in einem abstrakten Gesetz unbedingt Abstand genommen werden.

Von einem verpflichtenden Einsatz von Systemen zur Angriffserkennung im industriellen Umfeld der Energie- und Wasserwirtschaft ist aus diesen Gründen abzusehen. Die Absätze § 8a Abs. 1a BSIG-E und § 11 Abs. 1d EnWG sollten gestrichen werden.

3. Bußgeldvorschriften nach § 14 BSIG-E

Vorsätzliche oder fahrlässige Verstöße gegen Pflichten aus dem BSIG sollen mit Geldbußen von bis zu 2 Mio. €, 1 Mio. € oder 100.000 € geahndet werden, je nachdem, welche Verstöße begangen wurden. Dabei wird auf § 30 Absatz 2 Satz 3 des Gesetzes über Ordnungswidrigkeiten (OWiG) verwiesen. Demzufolge kann das Höchstmaß der Geldbuße verzehnfacht werden. In der Konsequenz kann das maximale Sanktionsmaß also auf 20 Mio. € bei schwerwiegenden Verstößen angehoben werden. Das entspricht einer Erhöhung des heutigen Bußgeld-Höchstmaßes um das bis zu 200-fache.

Ein derart enormes Sanktionsmaß ist weder sach- noch verhältnisgemäß und ist einer guten und vertrauensvollen Zusammenarbeit zwischen Betreibern und dem Bundesamt abträglich. Es ist nicht zielführend und kann gewünschten Investitionen in die Informationssicherheit entgegenwirken, wenn stattdessen für unverhältnismäßige Sanktionsrisiken umfangreiche Rückstellungen gebildet werden müssen. *Der Verweis auf § 30 Absatz 2 Satz 3 OWiG innerhalb der Bußgeldvorschriften sollte daher ersatzlos entfallen.*

4. Gefahr der Doppelregulierung durch § 2 Abs. 14

Der Gesetzentwurf führt in § 2 Abs. 14 den Begriff des „Unternehmen im besonderen öffentlichen Interesse“ ein. Hiermit sind insbesondere große Unternehmen gemeint, die zwar keine Betreiber Kritischer Infrastrukturen im Sinne der BSI-KritisV sind, die aber dennoch von erheblicher Bedeutung sind, weil ihr Ausfall oder ihre Beeinträchtigung erhebliche volkswirtschaftliche Schäden zur Folge hätte. Unternehmen, die bereits als KRITIS-Betreiber erfasst sind, sollen von dieser Regelung zwar ausgenommen sein. Nichtsdestotrotz besteht die Gefahr einer Doppelregulierung von Unternehmen der Energie- und Wasserwirtschaft.

Insbesondere große Unternehmen der Energiewirtschaft zählen ebenfalls zu den größten Unternehmen in Deutschland. Die relevanten Unternehmensteile sind jedoch (zum Teil über Tochtergesellschaften) bereits als Betreiber Kritischer Infrastrukturen erfasst, da diese Unternehmensteile Energieversorgungsnetze und/oder Energieanlagen betreiben. Im Sinne der internationalen Wettbewerbsfähigkeit deutscher der Unternehmen der Energiewirtschaft sollte eine Doppelregulierung als Betreiber Kritischer Infrastruktur und Unternehmen im besonderen öffentlichen Interesse ausgeschlossen werden. *Im Gesetzestext sollte demnach eindeutig ausgeschlossen werden, dass Unternehmen, die Betreiber einer Kritischen Infrastruktur sind, zusätzlich als Unternehmen im öffentlichen Interesse reguliert werden.*

Ansprechpartner

Yassin Bendjebbour
Betriebswirtschaft | Steuern | Digitalisierung
Telefon: +49 30 300199-1529
yassin.bendjebbour@bdew.de

Berlin, 10. Dezember 2020

bdew
Energie. Wasser. Leben.

BDEW Bundesverband der Energie- und Wasserwirtschaft e. V.
Reinhardtstraße 32
10117 Berlin

www.bdew.de

Stellungnahme

zu einem „Zweiten Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme“

im Zuge der Verbändeanhörung auf Basis des „Diskussionsentwurfs“ vom 1. Dezember 2020

Version: 1.0

Inhalt

Vorbemerkungen 2
Zu den Forderungen im Kern 5
Zu den Forderungen im Einzelnen 6
Artikel 1 Änderung des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) 6
Artikel 4 Änderung des Gesetzes über die Elektrizitäts- und Gasversorgung (EnWG) 19

Vorbemerkungen

Das Bundesministerium des Innern, für Bau und Heimat (BMI) hat am 9. Dezember 2020 mit einem Entwurf eines „Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme“, kurz genannt IT-Sicherheitsgesetz 2.0 (IT-SiG 2.0) die Verbändeanhörung eröffnet und bittet um Stellungnahme bis zum 10. Dezember 2020. Aufgrund der Kürze der Zeit nimmt der BDEW mit dem vorliegenden Dokument zu dem „Diskussionsentwurf“ in der Fassung vom 1. Dezember 2020 Stellung.

Wir begrüßen die Überarbeitung und Weiterentwicklung des Ordnungsrahmens zum Schutz Kritischer Infrastrukturen. Die Bedeutung von sicheren informationstechnischen Systemen für die Aufrechterhaltung der Energie- und Wasserver- bzw. -entsorgung ist elementar. Gleichermaßen ist zu beobachten, dass Bedrohungen aus dem digitalen Raum einerseits längst keine Fiktion mehr sind, andererseits stetig in ihrer Qualität und Häufigkeit zunehmen.

Wir stehen daher zu dem Ziel, die Informationssicherheit Kritischer Infrastrukturen weiter zu erhöhen. Mit dem vorliegenden Gesetzentwurf strebt das BMI jedoch eine deutliche Erhöhung der Pflichten von Betreibern Kritischer Infrastrukturen an, die massive wirtschaftliche Auswirkungen auf die betroffenen Unternehmen haben können. Mit der Einführung des IT-SiG wurde gesetzlich verankert, dass die etablierten Cyber- und IT-Sicherheitsmaßnahmen regelmäßig auf ihre Wirksamkeit wissenschaftlich überprüft sowie evidenzbasiert und im Dialog mit den betroffenen Kreisen weiterentwickelt werden. Es ist aus Sicht der Energie- und Wasserwirtschaft nicht nachvollziehbar, dass das BMI – trotz des nunmehr zweijährigen Zeitraums zur Erarbeitung des vorliegenden Entwurfs – nicht seiner gesetzlich verankerten Pflicht zu Evaluierung nachgekommen ist. Stattdessen wirkt das BMI aus Sicht der Energie- und Wasserwirtschaft auf eine überstürzte Verabschiedung des Gesetzentwurfs hin, ohne den betroffenen Kreisen eine angemessene Frist einzuräumen, um sich auf Basis eines offiziellen Entwurfs zu den komplexen Sachverhalten, die innerhalb des Gesetzgebungsverfahrens diskutiert werden, in angemessener Tiefe äußern zu können.

Mit dem UP KRITIS steht eine verlässliche und vertrauensvolle Struktur zur Zusammenarbeit zwischen staatlichen Stellen und der Wirtschaft zur Verfügung, um die Erfahrungen der letzten

Jahre kritisch reflektieren und sinnstiftend weiterentwickeln zu können. Der BDEW steht für die deutsche Energie- und Wasserwirtschaft für einen Dialog und für eine mit dem nötigen Fingerspitzengefühl und Augenmaß fortgeführte Weiterentwicklung jederzeit und gerne bereit.

Mit Blick auf die Inhalte des vorliegenden „Diskussionsentwurfs“ befürworten wir ausdrücklich, dass Hersteller von IT-Produkten und Anbieter digitaler Dienste zukünftig verpflichtet werden sollen, ihren Beitrag zum Schutz von Kritischen Infrastrukturen zu leisten. Das ist ein erheblicher Schritt nach vorne. Denn nur durch eine vertrauensvolle Kooperation zwischen Herstellern und Betreibern kann die Sicherheit von in der Energie- und Wasserwirtschaft eingesetzten Komponenten und Prozessen im Sinne des Regelungsziels effizient erhöht werden.

Zur Gewährleistung eines hohen Niveaus der Informationssicherheit sind die Betreiber Kritischer Infrastrukturen ebenfalls auf die Unterstützung des Bundesamts für Sicherheit in der Informationstechnik (Bundesamt, BSI) angewiesen. Aus diesem Grund sollten die Aufgaben, Zuständigkeiten und Befugnisse des Bundesamts dahingehend gesetzlich verankert werden, den Betreibern die betreffenden Informationen zu Bedrohungen aus dem digitalen Raum bereitzustellen, ohne dass vage formulierte Sicherheitsinteressen dem im Wege stehen. Die Fortführung des bewährten risikobasierten Ansatzes der Informationssicherheit stellt sicher, dass den Unternehmen der Energie- und Wasserwirtschaft für die Umsetzung der gesetzlichen Vorgaben ausreichend Gestaltungsspielräume unter Maßgabe der Wirtschaftlichkeit und Verhältnismäßigkeit eingeräumt werden.

Die im vorliegenden „Diskussionsentwurf“ angedachten Rechte und Pflichten von Betreibern Kritischer Infrastrukturen werden zu erheblichen Aufwänden in den betroffenen Unternehmen führen. Daher fordern wir, den Erfüllungsaufwand der Wirtschaft zur Umsetzung der Vorschriften des ITSiG 2.0 bezüglich der Verpflichtungen zur Meldung, Information sowie Speicherung von Daten zu minimieren. Darüber hinaus ist ein zusätzlicher laufender Erfüllungsaufwand, der durch das Regelungsvorhaben entsteht, mittels geeigneten Entlastungs- oder Refinanzierungsmaßnahmen zu kompensieren.

Des Weiteren weisen wir zu dem Entwurf vom 9. Dezember 2020 ergänzend und nicht abschließend im Folgenden darauf hin:

› Die Bundesregierung plant, diverse Übergangsfristen zur Umsetzung von Vorgaben, wie z.B. der Registrierung neuer Anlagen, zu streichen bei gleichzeitiger Verschärfung von Sanktionsmechanismen, die nicht mehr nur bei fahrlässigem oder vorsätzlichem Handeln verhängt wer-den können. Von diesem Zusammenspiel von gestrichenen Übergangs-fristen und unmittelbaren Sanktionstatbeständen geht ein hohes Risiko von existenzgefährdenden Bußgeldern für betroffene Unternehmen aus, die bereits aufgrund von Bagatell-Verstößen verhängt werden können. Wir fordern die Bundesregierung auf, den Gesetzentwurf im Sinne der Verhältnismäßigkeit von Bußgeldern zu Verstößen zu über-arbeiten.

- Von einer Einführung von Pflichten zur Umsetzung spezifischer technischer Maßnahmen in einem abstrakten Gesetz sollte unbedingt Ab-stand genommen werden. Der Entwurf enthält Anforderungen technischer Art, die mit der Realität der Praxis wenig gemeinsam haben. Die Pflicht zur Umsetzung würde betroffene Kreise vor unklare und zum Teil nicht lösbare Herausforderungen stellen, weitere Gefährdungen mit sich bringen und in Konsequenz zu erheblicher Rechtsunsicherheit führen. Es ist nicht nachvollziehbar, wie z.B. Systeme zur Angriffserkennung eingetretene Störungen beseitigen können. Auch können in-formationstechnische Systeme nicht eigenständig Bedrohungen vermeiden. Sachfremde Anforderungen sollten aus dem Gesetzestext entfernt werden.
- Die unvermittelte Aufnahme des § 10 Absatz 6 erschließt sich uns nicht. Aufgrund der fehlenden Begründung können weder Sinn und Zweck noch die Implikationen für den Betrieb von informationstechnischen Systemen der Betreiber Kritischer Infrastrukturen abgeschätzt werden. Es ist davon auszugehen, dass die Befugnis des Bundesinnen-ministeriums zu einem weitreichenden Eingriff führen würde.

Zu den Forderungen im Kern

Zum „Diskussionsentwurf“ eines IT-Sicherheitsgesetzes 2.0 gibt der BDEW zur beabsichtigten Stärkung der Sicherheit informationstechnischer Systeme zu bedenken, dass:

- von einer Ausweitung der Regelungen des § 9b auf die Sektoren Energie und Wasser dringend abzuraten ist. Die Einführung einer Zertifizierungspflicht von „kritischen Komponenten“ in bestehenden Infrastrukturen im energie- und wasserwirtschaftlichen Umfeld ist eine hochsensible Angelegenheit. Die Auswirkungen sind in dem vorherrschenden, komplexen Einsatzumfeld vielfältig und nur schwer endgültig zu bemessen. Die Definition von „kritischen Komponenten“ nach § 2 Absatz 13 kann in der vorliegenden Formulierung einzig in Telekommunikationsnetzen Anwendung finden. Daher ist die Einführung einer Zertifizierungspflicht für in weiteren Sektoren aus dem Gesetz zu streichen.
- von einem verpflichtenden Einsatz von Systemen zur Angriffserkennung im industriellen Umfeld der Energie- und Wasserwirtschaft abzusehen ist. Eine Umsetzung in prozess- und leittechnischen Einrichtungen ist gegenwärtig nach allgemeinem Stand der Technik nur äußerst aufwändig und höchstwahrscheinlich nicht mit dem angestrebten Sicherheitszugewinn umsetzbar. Die Pflicht zur Speicherung sollte 12 Monate nicht übersteigen. Aufgrund der hohen Aufwände ist eine Umsetzungsfrist von mindestens zwei Jahren unerlässlich.
- in § 14 Bußgeldvorschriften der Verweis auf § 30 Absatz 2 Satz 3 OWiG ersatzlos gestrichen wird. Nur unter Berücksichtigung der vorgeschlagenen Streichung kann die Energie- und Wasserwirtschaft die erhöhten Bußgeldvorschriften über 2 Mio. €, 1 Mio. € bzw. 100.000 € als sachgemäß und verhältnismäßig erachten.
- die Gefahr einer Doppelregulierung als Unternehmen im besonderen öffentlichen Interesse für Unternehmen der Energie- und Wasserwirtschaft besteht, die beispielsweise Energieversorgungsnetze und/oder Energieanlagen (über Tochtergesellschaften) betreiben und zu den größten Unternehmen in Deutschland zählen.
- das Bundesamt gesetzlich dazu verpflichtet werden sollte, erlangte Informationen zu Sicherheitsrisiken zu verarbeiten und betroffene Kreise über alle relevanten Erkenntnisse zu informieren.
- im Falle einer Detektion von Sicherheitsrisiken für die IT-Sicherheit eines Betreibers der betroffene Betreiber ohne Ausnahmen umgehend zu informieren ist. Beim Einsatz von Honeypots muss ausgeschlossen werden, dass Kennungen von informationstechnischen Systemen von Betreibern Kritischer Infrastrukturen durch das Bundesamt genutzt werden. Wir begrüßen, dass weitergehende, invasive Maßnahmen durch das Bundesamt explizit ausgeschlossen werden sollen.
- die Entwicklung und Veröffentlichung von sicherheitstechnischen Anforderungen nach § 3 Absatz 1 Satz 2 Nummer 20 durch das Bundesamt nicht in einen nationalen Alleingang münden darf. Der Stand der Technik sollte möglichst auf Basis international anerkannter Normen und Standards definiert werden, an deren Erarbeitung die betroffenen Sektoren Kritischer Infrastrukturen und deren Wirtschafsverbände hinreichend beteiligt sind.

Zu den Forderungen im Einzelnen

Artikel 1 Änderung des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSIG)

Zu § 2 Absatz 13 Definition „kritische Komponente“

Worum geht es?
Es sollen sogenannte „kritische Komponenten“ eingeführt werden. Dies sollen IT-Produkte sein, die von Betreibern von öffentlichen Telekommunikationsnetzen oder Anbietern öffentlich zugänglicher Telekommunikationsdienste eingesetzt werden. Für derartige Betreiber werden „kritische Komponenten“ durch den Katalog für Sicherheitsanforderungen nach § 109 Absatz 6 des Telekommunikationsgesetzes näher bestimmt. Alle übrigen „kritischen Komponenten“ werden gesetzlich festgelegt.

Einschätzung:
Die Einführung einer Definition von „kritischen Komponenten“ dient in Verbindung mit Artikel 1 § 9b BSIG der Verpflichtung von Herstellern besagter Komponenten. In der vorliegenden Fassung liegt jedoch der Schluss nahe, dass die Aufwände im Kontext des Regelungsziels auf Seiten der Anwender solcher Komponenten verortet sein werden, also bei den Betreibern öffentlicher Telekommunikationsnetze oder bei Anbietern öffentlich zugänglicher Telekommunikationsdienste. Es ist gängige Praxis, dass Betreiber Kritischer Infrastrukturen in der Energie- und Wasserwirtschaft die für die Erbringung der kritischen Dienstleistung wesentlichen Komponenten auf Basis des risikobasierten Ansatzes u.a. der IT-Sicherheitskataloge nach § 1a bzw. 1b EnWG eigenständig bestimmen. Im Falle der Einführung einer Zertifizierungspflicht für „kritische Komponenten“ in den Sektoren Energie und Wasser darf nicht daran gerüttelt werden. Die angedachte Definition dient im spezifischen Kontext nur dem Regelungsziel, die Vertrauenswürdigkeit von Herstellern von „kritischen Komponenten“ zu adressieren. Lediglich die jeweiligen Betreiber können die Kritikalität einer Komponente bzw. eines Komponententyps in Abhängigkeit von dem spezifischen Einsatzumfeld bewerten. Die Einführung einer Zertifizierungspflicht im Sektor Energie und Wasser würde eine unverhältnismäßige und wirtschaftlich äußerst aufwändige Bürokratisierung mit zweifelhaftem Wert für die operative IT-Sicherheit darstellen.

BDEW-Petitum:
Wir raten eindringlich von der Einführung einer Zertifizierungspflicht für „kritische Komponenten“ in den Sektoren Energie und Wasser ab. Satz 2 in folgendem Passus sollte daher gestrichen werden:

> *„(13) Kritische Komponenten im Sinne dieses Gesetzes werden für Betreiber nach § 8d Absatz 2 Nummer 1 durch den Katalog von Sicherheitsanforderungen nach § 109 Absatz 6 des Telekommunikationsgesetzes näher bestimmt. ~~Alle übrigen kritischen Komponenten werden gesetzlich festgelegt.~~“*

Zu § 2 Absatz 14 - Definition Unternehmen im besonderen öffentlichen Interesse

Worum geht es?

Das IT-Sicherheitsgesetz soll auf weitere Teile der Wirtschaft ausgeweitet werden. Zu diesem Zweck soll eine neue Kategorie eingeführt werden, die Unternehmen im besonderen öffentlichen Interesse umfasst, die nicht Betreiber Kritischer Infrastrukturen nach Absatz 10 sind. Zu diesen gehören

1) nach Nummer 1 Rüstungshersteller sowie Hersteller von IT-Produkten für die Verarbeitung staatlicher Verschlusssachen,
2) Unternehmen, die nach ihrer inländischen Wertschöpfung zu den größten Unternehmen in Deutschland gehören und daher von erheblicher volkswirtschaftlicher Bedeutung für die Bundesrepublik Deutschland sind,
3) sowie Betreiber von Betriebsbereichen der oberen Klasse im Sinne der Zwölften Verordnung zur Durchführung des Bundes-Immissionsschutzgesetzes (Störfallverordnung).

Die neue Kategorie der Unternehmen im besonderen öffentlichen Interesse habe zwar eine große Bedeutung in Bezug auf die IT-Sicherheit in Deutschland, jedoch sei diese im direkten Vergleich zu Betreibern Kritischer Infrastrukturen deutlich abgestuft. Sowohl die neu einzuführende Definition für Unternehmen im besonderen öffentlichen Interesse als auch die sich daraus ergebenden Rechtsfolgen für die betroffenen Unternehmen sollen nicht mit denen von Betreibern Kritischer Infrastrukturen vergleichbar sein. Um Unternehmen, die wegen ihrer Eigenschaft als Betreiber einer Kritischen Infrastruktur bereits höheren Schutzanforderungen unterliegen, nicht unnötig zu belasten, soll ein Unternehmen nicht als Unternehmen im besonderen öffentlichen Interesse im Sinne dieses Gesetzes gelten, wenn es Betreiber einer Kritischen Infrastruktur ist (vgl. § 2 Absatz 14).

Einschätzung:

Die Ausweitung des IT-Sicherheitsgesetzes auf weitere Teile der Wirtschaft geht verschärfend über die Vorgaben der EU-Richtlinie zur Gewährleistung einer hohen Netzwerk- und Informationssicherheit hinaus. Es ist jedoch zu begrüßen, dass Betreiber Kritischer Infrastrukturen nicht

zusätzlich als Unternehmen im besonderen öffentlichen Interesse erfasst werden sollen. Aufgrund der uneindeutigen Formulierung, welche Unternehmen aufgrund ihrer inländischen Wertschöpfung zu den größten Unternehmen in Deutschland gehören, kann es dennoch zu einer Doppelregulierung kommen. Insbesondere große Unternehmen der Energiewirtschaft zählen ebenfalls zu den größten Unternehmen in Deutschland, gemessen an ihrer summierten inländischen Wertschöpfung. Die relevanten Unternehmensteile sind jedoch (zum Teil über Tochtergesellschaften) bereits als Betreiber Kritischer Infrastrukturen erfasst, da diese Unternehmensteile Energieversorgungsnetze und/oder Energieanlagen betreiben. Es sollte daher eingehend geprüft werden, ob der Besitz von Unternehmen, die Betreiber einer Kritischen Infrastruktur sind, ein hinreichendes Merkmal für ein Unternehmen im öffentlichen Interesse sein kann.

BDEW-Petitum:

Wir weisen auf die Gefahr einer Doppelregulierung von Unternehmen der Energie- und Wasserwirtschaft hin, die beispielsweise Energieversorgungsnetze und/oder Energieanlagen, zum Teil über Tochtergesellschaften, betreiben lassen und aufgrund ihrer summierten inländischen Wertschöpfung zu den größten Unternehmen in Deutschland nach §§ 44 Absatz 1 GWB (sog. Hauptgutachten) zählen. Der BDEW steht jederzeit zur Verfügung, in der Ausgestaltung der Rechtsverordnung nach § 10 Absatz 5 mitzuwirken und empfiehlt, die Identifizierung von „Unternehmen im öffentlichen Interesse“ ohne eine Vermischung mit Betreibern Kritischer Infrastrukturen vorzunehmen.

Zu § 3 Absatz 1 Satz 2 Nummer 20 - Entwicklung und Veröffentlichung eines Stands der Technik bei sicherheitstechnischen Anforderungen an IT-Produkte

Worum geht es?

Das Bundesamt soll zusätzlich zu bestehenden Aufgaben u.a. sicherheitstechnische Anforderungen an IT-Produkte entwickeln und veröffentlichen können.

Einschätzung:

Betreiber Kritischer Infrastrukturen sind nach § 8a BSIG zur Umsetzung von technischen und organisatorischen Maßnahmen nach dem Stand der Technik verpflichtet. Die Betreiber Kritischer Infrastrukturen sind daher als unmittelbar Betroffene bei der Entwicklung eines Stands der Technik bei sicherheitstechnischen Anforderungen an IT-Produkte unbedingt einzubeziehen, analog zu Beteiligungsmöglichkeiten in der nationalen, europäischen und internationalen Normung.

BDEW-Petitum:

Die sicherheitstechnischen Anforderungen sollten sich auf Vorgaben zu Rahmenbedingungen und informationstechnischen Schutzzielen begrenzen, um betriebswirtschaftlich unverhältnis-

mäßig teuren und ggf. praktisch wenig wirksamen sicherheitstechnischen Anforderungen an IT-Produkte vorzubeugen. Der Stand der Technik sollte auf Basis anerkannter Normen und Standards, an deren Erarbeitung alle betroffenen Kreise beteiligt sind, definiert werden. Es darf keine Abkehr von etablierten Verfahren geben. Zertifizierungen, die nach dem Stand der Technik anderer kompetenter Organisationen für Informationssicherheit erfolgen, sind ebenfalls anzuerkennen.

Ferner sollte sich der Stand der Technik durch marktreife Produkte umsetzen lassen. Eine Norm oder ein Standard, für den es noch kein Produkt gibt, welches sich wirtschaftlich einsetzen lässt, kann nicht umgesetzt werden.

Wir regen an, den Passus zu ergänzen:

> *"20. Entwicklung von Rahmenbedingungen sowie Schutzzielen unter Einbezug der betroffenen Betreiber Kritischer Infrastrukturen und Veröffentlichung eines Stands der Technik bei sicherheitstechnischen Anforderungen an marktverfügbare IT-Produkte unter Berücksichtigung von bestehenden, anerkannten Normen und Standards."*

Zu § 4b - Allgemeine Meldestelle für die Sicherheit in der Informationstechnik

Worum geht es?

Der vorliegende § 4b regelt die Rechte und Pflichten des Bundesamts als allgemeine Meldestelle für die Sicherheit in der Informationstechnik. Die zentrale Sammlung und Auswertung von Informationen zu Sicherheitslücken, Schadprogrammen und IT-Sicherheitsvorfällen zur Einschätzung der IT-Sicherheitslage ist vor diesem Hintergrund eine elementare Aufgabe.

Einschätzung:

Betreiber Kritischer Infrastrukturen sind auf die kurzfristige Bereitstellung von Informationen zu allgemeinen wie auch sektorspezifischen Bedrohungen und Gefährdungslagen – besonders durch staatliche Stellen – angewiesen, um zu jeder Zeit einen sicheren Betrieb ihrer Kritischen Infrastruktur im Sinne des Gesetzgebers gewährleisten zu können. Dementsprechend sollte das Bundesamt gesetzlich dazu verpflichtet werden, erlangte Informationen zu verarbeiten und betroffene Kreise umgehend über relevante Erkenntnisse zu informieren.

BDEW-Petitum:

Wir regen an, den Passus wie folgt zu ändern:

> *(3) Das Bundesamt hat die gemäß Absatz 2 gemeldeten Informationen zu verarbeiten, um: …".*

Zu § 7b - Detektion von Sicherheitsrisiken für die Netz- und IT-Sicherheit und von Angriffsmethoden

Worum geht es?

Das Bundesamt kann Maßnahmen zur Detektion und Auswertung von Schadprogrammen, Sicherheitslücken und anderen Sicherheitsrisiken an den Schnittstellen öffentlich erreichbarer informationstechnischer Systeme zu öffentlichen Telekommunikationsnetzen Maßnahmen (Portscans) durchführen, wenn Tatsachen die Annahme rechtfertigen, dass diese ungeschützt im Sinne des Absatzes und dadurch in ihrer Sicherheit oder Funktionsfähigkeit gefährdet sein können.

Ein informationstechnisches System im Sinne des Absatzes 1 ist ungeschützt im Sinne des Absatzes 1, wenn auf diesem öffentlich bekannte Sicherheitslücken bestehen oder wenn auf Grund sonstiger offensichtlich unzureichender Sicherheitsvorkehrungen unbefugt von Dritten auf das System zugegriffen werden kann.

Die Verantwortlichen oder der betreibende Dienstleister des jeweiligen Netzes oder Systems sind zu benachrichtigen, wenn sie bekannt sind oder ihre Identifikation ohne unverhältnismäßige weitere Ermittlungen möglich ist und überwiegende Sicherheitsinteressen nicht entgegenstehen.

Das Bundesamt darf Systeme und Verfahren einsetzen, welche einem Angreifer einen erfolgreichen Angriff vortäuschen, um Schadprogramme und andere Angriffsmethoden zu erheben und auszuwerten. Das Bundesamt darf die hierzu erforderlichen Daten verarbeiten.

Einschätzung:

Die vorgesehene Befugnis des Bundesamts zur Detektion von Sicherheitsrisiken für die Netz- und IT-Sicherheit und von Angriffsmethoden ist grundsätzlich zu begrüßen. Die Maßnahmen müssen sich auf die Detektion begrenzen. Die Durchführung von invasiven Maßnahmen ist mit Absatz Satz 2 ausgeschlossen.

Es ist zu beachten, dass eine unautorisierte Detektion und Auswertung von Sicherheitslücken und anderen Sicherheitsrisiken in informationstechnischen Systemen von Betreibern Kritischer Infrastrukturen, einen sicheren Systembetrieb empfindlich stören kann und im Endeffekt die Erbringung einer kritischen Dienstleistung gefährden könnte. Daher ist es ratsam, betroffene Betreiber in die Maßnahmen zur Detektion von Schadprogrammen, Sicherheitslücken und weitere Sicherheitsrisiken rechtzeitig einzubeziehen, u.a. durch eine Vorabinformation und Bereitstellung der genutzten Kennungen des Bundesamts.

BDEW-Petitum:

Sollten dem Bundesamt Sicherheitsrisiken für die Netz- und IT-Sicherheit eines Betreibers einer Kritischen Infrastruktur bekannt werden, ist der betroffene Betreiber umgehend zu informieren. Ein Verweis auf generisch definierte, überwiegende Sicherheitsinteressen darf eine Benachrichtigung nicht verzögern oder verhindern. Es ist zu begrüßen, dass das Bundesamt

den betroffenen Betreibern Hinweise zu Abhilfemöglichkeiten geben soll. In jedem Fall sollte im Vorfeld von geplanten Detektionsmaßnahmen der betroffene Betreiber der Kritischen Infrastruktur durch das Bundesamt über die eingerichtete Kontaktstelle informiert werden inkl. der Bereitstellung der genutzten Kennungen (oder anderer eindeutiger Identifikatoren) des Bundesamtes.

Der geplante Einsatz von Systemen und Verfahren, welche einem Angreifer einen erfolgreichen Angriff vortäuschen (sogenannte „Honeypots“), ist grundsätzlich zu begrüßen. Es muss allerdings ausgeschlossen werden, dass Kennungen und Adressen von informationstechnischen Systemen von Betreibern Kritischer Infrastrukturen durch das Bundesamt zu diesem Zweck genutzt werden.

Demnach regen wir folgende Ergänzung und Konkretisierung des Passus an:

> *„§ 7b Detektion von Sicherheitsrisiken für die Netz- und IT-Sicherheit und von Angriffsmethoden*
>
> *[…]*
>
> *(3) Die für das informationstechnische System Verantwortlichen sind vor Maßnahmen gemäß Absatz 1 zu benachrichtigen, sofern diese Betreiber Kritischer Infrastrukturen oder Unternehmen im besonderen öffentlichen Interesse sind. Wird durch Maßnahmen gemäß Absatz 1 eine Sicherheitslücke oder ein anderes Sicherheitsrisiko eines informationstechnischen Systems erkannt ~~und stehen überwiegende Sicherheitsinteressen nicht entgegen~~, sind die für das informationstechnische System Verantwortlichen darüber zu informieren. Das Bundesamt soll dabei auf bestehende Abhilfemöglichkeiten hinweisen. Sind dem Bundesamt die Verantwortlichen nicht bekannt oder ist ihre Identifikation nur mit unverhältnismäßigem Aufwand möglich und stehen überwiegende Sicherheitsinteressen nicht entgegen, ist hilfsweise der betreibende Dienstleister des jeweiligen Netzes oder Systems unverzüglich zu benachrichtigen. Das Bundesamt unterrichtet die Bundesbeauftragte oder den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit jeweils bis zum 30. Juni des Folgejahres über die Anzahl der gemäß Absatz 1 ergriffenen Maßnahmen.*
>
> *(4) Das Bundesamt darf zur Erfüllung seiner Aufgaben Systeme und Verfahren einsetzen, welche einem Angreifer einen erfolgreichen Angriff vortäuschen, um den Einsatz von Schadprogrammen oder andere Angriffsmethoden zu erheben und auszuwerten. Das Bundesamt darf dabei die zur Auswertung der Funktionsweise der Schadprogramme und Angriffsmethoden erforderlichen Daten verarbeiten. Die Verwendung von Kennungen und Adressen von informationstechnischen Systemen von Betreibern Kritischer Infrastrukturen oder Unternehmen im besonderen öffentlichen Interesse durch das Bundesamt ist hiervon explizit ausgenommen, sodass jeglicher Bezug zu einer realexistierenden Infrastruktur unterlassen wird.*

Zu § 8a Absätze 1a und 1b - Systeme zur Angriffserkennung

Worum geht es?

Betreiber sollen im Rahmen technischer und organisatorischer Maßnahmen nach § 8a BSIG zusätzlich Systeme zur Angriffserkennung einsetzen. Betreibern wird dabei eine Übergangsfrist von maximal einem Jahr nach Inkrafttreten des Gesetzes gewährt. Die eingesetzten Systeme müssen geeignete Parameter bzw. Merkmale aus dem laufenden Betrieb kontinuierlich und automatisch erfassen und auswerten. Sie sollen dazu in der Lage sein, fortwährend Bedrohungen zu identifizieren und zu vermeiden sowie für eingetretene Störungen geeignete Beseitigungsmaßnahmen vorsehen. Dabei soll der Stand der Technik eingehalten werden. Organisatorische und technische Vorkehrungen sind angemessen, wenn der dafür erforderliche Aufwand nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung der betroffenen Kritischen Infrastruktur steht.

Betreiber Kritischer Infrastrukturen müssen für die Angriffserkennung und -nachverfolgung relevante nicht personenbezogene Daten, die beim Betrieb einer Kritischen Infrastruktur anfallen, mindestens vier Jahre speichern.

Einschätzung:

Der Einsatz von Systemen zur Angriffserkennung ist heute unter Betreibern Kritischer Infrastrukturen im Sinne der BSI-KritisV in der Energie- und Wasserwirtschaft insbesondere in Büronetzwerken weit verbreitet. Die Formulierung im Gesetzestext legt nahe, dass lediglich Systeme zur Angriffserkennung (Intrusion Detection) verpflichtend zum Einsatz kommen sollen. Systeme zur Angriffsbehandlung (Intrusion Prevention) befinden sich allerdings zum gegenwärtigen Zeitpunkt im Umfeld industrieller Prozess -und Automatisierungstechnik noch in einem unreifen Entwicklungsstand. Ihr Einsatz in Produktivnetzwerken würde zu einer Gefährdung der Versorgungsdienstleistung führen. Der Betrieb solcher Systeme erfordert umfassende zeitliche wie wissenstechnische Kapazitäten, da Meldungen zu Angriffen nur durch die manuelle Analyse hinsichtlich ihres Gefährdungspotenzials für die Erbringung einer kritischen Dienstleistung eingeordnet werden können. Nur nach einer solch qualifizierten Einordnung können solche Systeme eine Schutzwirkung im avisierten Einsatzumfeld entfalten.

Die Speicherfrist von für die Angriffserkennung relevanten nicht personenbezogenen Daten, die beim Betrieb einer Kritischen Infrastruktur anfallen, über mindestens vier Jahren würde zu erheblichen Herausforderungen und Aufwänden führen: Nicht personenbezogene Daten müssten von personenbezogenen Daten separiert und für die Archivierung aufbereitet werden. Es ist zu erwarten, dass die anfallenden Datenmengen umfassenden Speicherbedarf erzeugen würden. In der Begründung wird angesichts der Persistenz von spezifischen Angreifenden die Notwendigkeit einer langen Speicherfrist formuliert. Die Erfahrungen aus der Praxis zeigen, dass in derartigen Fällen zwischen den Zeitpunkten einer Infiltration und einem Datenabfluss bzw. Verschlüsselung, z.B. bei Ransomware, meist 140 bis 200 Tage liegen.

Sinnvoll erscheint ergänzend, dass das Bundesamt den Auftrag erhält und befähigt wird, die unterschiedlichen, am internationalen Markt erhältlichen Systeme zur Angriffserkennung zu prüfen und zu bewerten.

BDEW-Petitum:

Von einem verpflichtenden und flächendeckenden Einsatz von Systemen zur Angriffserkennung ist im industriellen Umfeld der Energie- und Wasserwirtschaft abzusehen. Eine Umsetzung in prozess- und leittechnischen Einrichtungen ist gegenwärtig nach allgemeinem Stand der Technik nicht zuverlässig realisierbar, da in diesem Umfeld spezifische Verfahren und spezielle informationstechnische Umgebungen vorherrschen. Die flächendeckende Einführung und der Betrieb derartiger Systeme ist in mehrfacher Weise aufwendig, die reibungslose und effiziente Funktionsweise ist abhängig von einer hohen Implementierungsqualität und ist nur durch umfangreiche Anpassungen der vorliegenden informationstechnischen Infrastrukturen der Unternehmen realisierbar. Der Einbau einer zusätzlichen, unsicheren Komponente in ein informationstechnisches System lässt zusätzlich neue Gefährdungen entstehen. Vor diesem Hintergrund ist aus Sicht der Energie- und Wasserwirtschaft ein Einsatz derartiger Systeme in prozess- und leittechnischen Einrichtungen im Sinne des Gesetzes im Angesicht des erforderlichen Aufwands nicht angemessen, da das Interesse an einem verlässlichen und stabilen Betrieb Kritischer Infrastrukturen den Mehrwert derartiger Systeme überwiegt. Sollte es zur Einführung einer Pflicht zum Einsatz derartiger Systeme kommen, ist angesichts des damit verbundenen hohen Aufwands eine Umsetzungsfrist von mindestens zwei Jahren notwendig.

Die Speicherfrist sollte im Kontext der Erfahrungen aus der Praxis auf maximal 12 Monate begrenzt werden, analog zur Pflicht des Bundesamts zur Verarbeitung und Speicherung von behördeninternen Protokollierungsdaten nach § 5a Absatz 2. Ein Angriffsversuch sollte nicht verpflichtend protokolliert werden müssen, da die Definition des Angriffsversuchs nicht klar ist und somit zu einem hohen Mehraufwand ohne konkreten Zusatznutzen führen wird.

Wir regen an, den Passus wie folgt umzuformulieren:

> *„(1a) Die Verpflichtung nach Absatz 1 Satz 1, angemessene organisatorische und technische Vorkehrungen zu treffen, umfasst spätestens zwei Jahre nach Inkrafttreten dieses Gesetzes auch den Einsatz von Systemen zur Angriffserkennung. Die eingesetzten Systeme zur Angriffserkennung müssen geeignete Parameter bzw. Merkmale aus dem laufenden Betrieb kontinuierlich und automatisch erfassen und auswerten. Sie sollten dazu in der Lage sein, fortwährend Bedrohungen zu identifizieren und zu vermeiden sowie für eingetretene Störungen geeignete Beseitigungsmaßnahmen vorsehen. Absatz 1 Satz 2 und 3 gelten entsprechend. Ein flächendeckender Einsatz von Systemen zur Angriffserkennung im Umfeld von informationstechnischen Systemen, die für die Erbringung einer kritischen Dienstleistung wesentlich sind, ist hiervon ausgenommen.*

Das Bundesamt prüft und bewertet die am Markt verfügbaren Systeme zur Angriffserkennung regelmäßig und spricht auf Anfrage Empfehlungen aus.

(1b) Betreiber Kritischer Infrastrukturen müssen für die Angriffserkennung und -nachverfolgung relevante nicht personenbezogene Daten, die beim Betrieb einer Kritischen Infrastruktur anfallen, maximal 12 Monate speichern."

Zu § 8b Absatz 4a - Zentrale Stelle für die Sicherheit in der Informationstechnik Kritischer Infrastrukturen

Worum geht es?

Während einer erheblichen Störung der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der informationstechnischen Systeme, Komponenten oder Prozesse von Betreibern Kritischer Infrastrukturen, die zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen führen können oder von Unternehmen im besonderen öffentlichen Interesse, die zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Erbringung der Wertschöpfung führen können bzw. die zu einem Störfall nach der Störfall-Verordnung in der jeweils geltenden Fassung führen können, kann das Bundesamt im Einvernehmen mit der jeweils zuständigen Aufsichtsbehörde des Bundes von den betroffenen Betreibern bzw. Unternehmen die Herausgabe der zur Bewältigung der Störung notwendigen Informationen, einschließlich personenbezogener Daten, verlangen.

Einschätzung:

In einem anhaltenden oder sich ausweitenden Störungsausfall ist der Wunsch der Aufsichtsbehörde nach umfangreichen Informationen verständlich. Dennoch möchten wir darauf hinweisen, dass bereits für eine lediglich rudimentäre Einordnung der eingeforderten Informationen durch unbeteiligte Externe ein erhebliches Wissen über die Spezifika des jeweiligen Umfelds betroffener informationstechnischer Systeme notwendig ist. Es scheint uns daher unwirksam, dem Bundesamt alle zur Bewältigung einer Störung notwendigen Informationen aushändigen zu müssen, inklusive sämtlicher dazu notwendigen Benutzerkennungen, Passwörter und dazugehöriger Betriebsdokumentationen.

Störungen sind für Betreiber Kritischer Infrastrukturen schon heute meldepflichtig. Uns sind gegenwärtig keine Beispiele seit Einführung der Meldepflicht bekannt, in denen eine solche Übermittlung, wie die hier geplante, eine Störungsbehebung beschleunigt hätte. Vielmehr erscheint es uns angebracht, die Kooperation zwischen Betreibern und dem Bundesamt weiter vertrauensvoll zu vertiefen.

BDEW-Petitum:

Wir regen an, den Passus zu streichen. Ergänzend könnten die Vorgaben zur Meldepflicht anforderungsgerecht und im Dialog mit den Betreibern präzisiert werden.

~~*„(4a) Während einer erheblichen Störung gemäß Absatz 4 Satz 1 Nummer 2, § 8f Absatz 7 Nummer 2 oder § 8f Absatz 8 Nummer 2 kann das Bundesamt im Einvernehmen mit der jeweils zuständigen Aufsichtsbehörde des Bundes von den betroffenen Betreibern Kritischer Infrastrukturen oder Unternehmen im besonderen öffentlichen Interesse die Herausgabe der zur Bewältigung der Störung not-wendigen Informationen einschließlich personenbezogener Daten verlangen.“*~~

Zu § 9b - Untersagung des Einsatzes kritischer Komponenten nicht vertrauenswürdiger Hersteller

Worum geht es?

Geplant ist die Einführung einer Garantieerklärung über die Vertrauenswürdigkeit von Herstellern von „kritischen Komponenten“ nach § 2 Absatz 13, in Sektoren, in denen eine gesetzliche Zertifizierungspflicht für „kritische Komponenten“ im Sinne dieses Gesetzes besteht. Gemäß Artikel 2 Änderung des Telekommunikationsgesetzes § 109 (2) Satz 4 soll dies zum gegenwärtigen Zeitpunkt ausschließlich für den Sektor Telekommunikation gelten. Für weitere Sektoren der Kritischen Infrastrukturen besteht derzeit keine gesetzliche Zertifizierungspflicht für „kritische Komponenten“. Der Einsatz von „kritischen Komponenten“, für die eine Zertifizierungspflicht besteht, soll durch den Betreiber einer Kritischen Infrastruktur gegenüber dem Bundesinnenministerium vor Einsatz angezeigt werden. Die Mindestanforderungen an eine Garantieerklärung sollen durch Allgemeinverfügung durch das Bundesinnenministerium festgelegt werden. Das Bundesinnenministerium kann den Einsatz einer Komponente, weiterer Komponenten eines spezifischen Typs sowie alle Komponenten eines Herstellers im Einvernehmen mit dem Bundesministerium für Wirtschaft und Energie und dem Auswärtigen Amt untersagen.

Einschätzung:

Die Energie- und Wasserwirtschaft begrüßt, dass im Zuge des Gesetzgebungsverfahrens Hersteller von IT-Produkten und „kritischen Komponenten“ hinsichtlich der Schutzziele Kritischer Infrastrukturen stärker in die Pflicht genommen werden sollen. Neben den Pflichten zur Kooperation zur Beseitigung von Schwachstellen, Störungen und Sicherheitsrisiken nach §§ 7a, 7c, 7d sowie 8b der von ihnen hergestellten IT-Produkte stellt der vorliegende § 9b eine erhebliche Verschärfung dar.

Die vorliegende Formulierung des Passus in Verbindung mit Artikel 2 Änderung des Telekommunikationsgesetzes § 109 Absatz 2 Satz 4 legt den Schluss nahe, dass der Anwendungsbereich ausschließlich auf Basis gesetzlicher Regelungen eine Zertifizierungspflicht im Telekommunikationssektor herbeiführen will. Die Einführung einer Garantieerklärung für „kritische Komponenten“ in weiteren Sektoren hätte in der vorgeschlagenen Form zusätzliche Aufwände auf Betreiberseite zur Folge: Von der Einholung einer Garantieerklärung für „kritische Komponenten“ über deren Administration bis zu den potenziellen wirtschaftlichen Folgeschäden

durch die Untersagung eines Komponenteneinsatzes müssten Betreiber die Auswirkungen tragen. Dazu würden der Aufwand und die Kosten für ggf. nötige Neuinstallationen zählen, die insbesondere bei Bestandsanlagen und anstehenden Teilprojekten eine große Unsicherheit nach sich ziehen würden.

Bezüglich einer möglichen Ausweitung auf weitere Sektoren der Kritischen Infrastrukturen neben dem Telekommunikationssektor weisen die Unternehmen der Energie- und Wasserwirtschaft darauf hin, dass bei der Vielzahl der heute von ihnen eingesetzten Komponenten staatliche Sicherheitsinteressen bzw. sicherheitspolitische Belange weder im Planungs- noch Herstellungszyklus, geschweige denn im Betriebs- und Entsorgungszyklus, berücksichtigt werden. Sollte eine solche Berücksichtigung aufgrund einer geänderten gesetzlichen Anforderung verpflichtend werden, sind nicht nur gewaltige Auswirkungen auf die Hersteller- und Lieferantenstruktur, sondern auch auf unternehmensinterne, kritische Geschäftsprozesse aller Betroffenen in der Energie- und Wasserwirtschaft zu erwarten. Zweckmäßige Investitionen, die auch zur Verbesserung der Informationssicherheit (z.B. Modernisierung von Teilen eines Leitsystems) führen würden, müssten vor diesem Hintergrund erneut und umfassend auf den Prüfstand gestellt und schlimmstenfalls abgesetzt werden. Die Investitionssicherheit wäre nicht gegeben aufgrund einer plötzlichen, außerhalb des Einflussbereichs eines Betreibers eintretenden ordnungsbehördlichen Untersagung. Daher müssen bereits im Einsatz befindliche Komponenten von der Neuregelung ausgenommen werden.

Die Einführung einer Zertifizierungspflicht von „kritischen Komponenten“ in bestehenden IT-Infrastrukturen im energie- und wasserwirtschaftlichen Umfeld ist eine hochsensible Angelegenheit. Die Auswirkungen sind in dem vorherrschenden, komplexen Einsatzumfeld vielfältig und nur schwer endgültig zu bemessen. Folgende Dynamiken sind dabei u.a. zu betrachten:

Der Markt für Hersteller und Lösungsanbieter von „kritischen Komponenten“, die in der Energie- und Wasserwirtschaft zum Einsatz kommen, ist überschaubar. Eine Zertifizierungspflicht hätte aller Voraussicht zur Folge, dass der Markt in seiner aktuell oligopolistischen Prägung zu einem Monopol werden könnte, d.h. auf wenige Hersteller weltweit eingeschränkt wäre. Vor dem Hintergrund der Bestrebungen um technologische Souveränität in der Europäischen Union muss aus Sicht des BDEW anhand der politischen und regulatorischen Rahmenbedingungen sichergestellt werden, dass jederzeit eine ausreichende Anzahl an vertrauenswürdigen europäischen Herstellern von „kritischen Komponenten“ garantiert ist, die eine gesetzeskonforme und vor allem belastbare Garantieerklärung ausstellen können. Eine Zertifizierungspflicht darf unter keinen Umständen in eine Abhängigkeit von Herstellern aus Nicht-EU-Staaten münden. Zudem ist davon auszugehen, dass eine Zertifizierungspflicht steigende Preise für „kritische Komponenten“ zur Folge haben würde, was wiederum eine nicht unerhebliche Wirkung auf die Marktpreise für die Versorgung mit Energie und Trinkwasser sowie für die Entsorgung von Abwasser entfalten würde.

Die Energie- und Wasserwirtschaft gibt darüber hinaus zu bedenken, dass eine alleinige Zertifizierungspflicht von einzelnen Komponenten nicht das Schutzniveau einer Anlage als Ganzes steigert. Nur durch das Zusammenspiel aller Komponenten, Anlagenteile und Ressourcen (Per-

sonal, Infrastrukturen, Prozesse, Verfahren und deren regelmäßige Pflege und Ineinanderwirken) kann ein hohes Schutzniveau erreicht werden. Der bestehende, risikobasierte Regulierungsansatz der IT-Sicherheitskataloge und branchenspezifischen Sicherheitsstandards (B3S) erfüllt diesen Anspruch.

BDEW-Petitum:

Von einer Ausweitung der Regelungen des § 9b auf die Sektoren Energie und Wasser ist dringend abzuraten. Die Aufwände für eine Einholung von Garantieerklärungen und deren potenziellen Ersatz in Folge einer Untersagung des Einsatzes sind erheblich und zum gegenwärtigen Zeitpunkt in den zu erwartenden mittel- und langfristigen Implikationen nur schwer abzuschätzen.

Der Passus sollte demzufolge dahingehend geändert werden, dass nicht Betreiber eine Garantieerklärung einholen und vorweisen müssen, sondern dass die Umsetzung dieser Vorgabe auf Seiten der hierfür originär verantwortlichen Hersteller verortet wird. So könnte beispielsweise das Bundesamt ein Register aller kritischen Komponenten und deren Hersteller führen, deren Einsatz eine Garantieerklärung nach § 9b für „kritische Komponenten“ nach § 2 Absatz 13 erfordern. Sollte eine Komponente in diesem Bundesamt-Register geführt werden, muss ein Hersteller gegenüber Betreibern einer Kritischen Infrastruktur ohne weitere Aufforderung, d.h. bei Auslieferung einer Komponente, eine Garantieerklärung ausstellen. Das Bundesamt sollte parallel die Möglichkeit erhalten, die Garantieerklärung auf deren Validität zu prüfen. Nach Ablauf der Frist von einem Monat gilt eine positive Bescheinigung der Garantieerklärung als erteilt. Der Betreiber zeigt daraufhin den Einsatz einer solchen Komponente gegenüber dem Bundesamt an und reicht die dazugehörige Garantieerklärung ein. Nach Ablauf der Frist von einem Monat gilt eine positive Bescheinigung der Garantieerklärung als erteilt.

Ferner regen wir an, die in Absatz 4 geregelte Untersagung des weiteren Betriebs einer „kritischen Komponente“ mittels einer verhältnismäßigen Frist zu konkretisieren. Bereits im Einsatz befindliche Komponenten müssen aufgrund der langen Lebensdauer Bestandsschutz erhalten. Im Falle einer Untersagung sind ausreichende Übergangsfristen für den Weiterbetrieb verbauter Komponenten vorzusehen, deren Länge den Einsatz von kompensierenden Sicherheitsmaßnahmen würdigt. Sollten qualifizierte Komponenten für einen Austausch nicht verfügbar sein, dann müssen ersatzweise Standardkomponenten über eine Betriebsbewährung und kompensierende Sicherheitsmaßnahmen qualifiziert werden können. Hier könnten die Erfahrungen aus der Regulierung kerntechnischer Anlagen herangezogen werden.

Zu § 14 - Bußgeldvorschriften

Worum geht es?
Vorsätzliche oder fahrlässige Verstöße gegen Pflichten aus dem BSIG sollen mit Geldbußen von bis zu 2 Mio. €, 1 Mio. € oder 100.000 € geahndet werden, je nachdem, welche Verstöße begangen wurden. Es wird auf § 30 Absatz 2 Satz 3 des Gesetzes über Ordnungswidrigkeiten (OWiG) verwiesen. Demzufolge kann das Höchstmaß der Geldbuße verzehnfacht werden. In der Konsequenz kann das maximale Sanktionsmaß auf 20 Mio. € bei schwerwiegenden Verstößen angehoben werden. Eine zuvor angedachte Verknüpfung mit weltweiten Jahresumsätzen eines Unternehmens wird nicht mehr vorgeschlagen.

Einschätzung:
Es ist begrüßenswert, dass sich das Strafmaß an einem europäischen Bußgeldrahmen orientiert. Die Energie- und Wasserwirtschaft ist sich ihrer Bedeutung für das Funktionieren des Gemeinwesens bewusst. Allerdings ist der Spagat aus ökonomischer und finanzieller Effizienzsteigerung bereits heute äußerst herausfordernd durch beispielsweise netzwirtschaftliche Anreizregulierung und den energiewirtschaftlichen Wettbewerb sowie die Übernahme staatlicher Aufgaben der Daseinsvorsorge durch privatwirtschaftliche Unternehmen.

Durch den Verweis auf § 30 Absatz 2 Satz 3 OWiG soll in letzter Konsequenz der Bußgeldrahmen in den Fällen des Absatzes 1 Nummer 1 Buchstabe a, Nummern 2, 9, 13, 14, 16, 17 und 18 enorm um das bis zu 200-Fache des derzeitigen Höchstmaßes erhöht werden. Diese Überlegung trägt den Bemühungen der Betreiber Kritischer Infrastrukturen in der Energie- und Wasserwirtschaft nicht Rechnung, die Informationssicherheit von Kritischen Infrastrukturen kontinuierlich zu stärken. Ein derart enormes Sanktionsmaß ist einer guten und vertrauensvollen Zusammenarbeit zwischen Betreibern und dem Bundesamt tendenziell abträglich, wodurch das in den letzten Jahren erarbeitete Vertrauensverhältnis nachhaltig gefährdet werden wird. Es ist anzuzweifeln, ob gewünschte Investitionen in die Informationssicherheit gefördert werden, wenn stattdessen für unverhältnismäßige Sanktionsrisiken umfangreiche Rückstellungen gebildet werden müssen.

Das Sanktionsmaß ist beispielsweise für Verstöße gegen die Vorgaben zur Speicherung von für die Angriffserkennung relevanten nicht personenbezogenen Daten, die beim Betrieb einer Kritischen Infrastruktur anfallen, nach § 8a Absatz 1b mit bis zu 20 Mio. € absolut unverhältnismäßig. Ein reiner Verstoß gegen die Vorgabe zur Speicherung ist bereits durch das heutige Strafmaß von maximal 100.000 € hinreichend bemessen.

BDEW-Petitum:
Der BDEW regt vor dem Hintergrund der im Grundgesetz angelegten Notwendigkeit der Einhaltung von Verhältnismäßigkeit bei staatlichen Maßnahmen an, den vorliegenden Passus wie folgt anzupassen:

> *(2) Die Ordnungswidrigkeit kann in den Fällen des Absatzes 1 Nummer 1 Buchstabe a, Nummern 2, 9, 13, 14, 16, 17 und 18 mit einer Geldbuße bis zu 2 Millionen Euro geahndet werden~~, auf § 30 Absatz 2 Satz 3 des Gesetzes über Ordnungswidrigkeiten wird verwiesen~~. Die Ordnungswidrigkeit kann in den Fällen des Absatzes 1 Nummer 1 Buchstabe*

b und Nummern 3, 5, 8, 10, 11, 12 und 15 mit einer Geldbuße bis zu 1 Million Euro geahndet werden. In den übrigen Fällen kann die Ordnungswidrigkeit mit einer Geldbuße bis zu 100.000 Euro geahndet werden.

Nur unter Berücksichtigung der vorgeschlagenen Streichung kann die Energie- und Wasserwirtschaft die Bußgeldvorschriften als sachgemäß und verhältnismäßig erachten.

Artikel 4 Änderung des Gesetzes über die Elektrizitäts- und Gasversorgung (EnWG)

Zu § 11 Absätze 1d, 1e und 1f EnWG

Worum geht es?

Durch die erwogene Änderung wird die in § 8a Absatz 1a BSIG neu einzuführende Pflicht für Betreiber Kritischer Infrastrukturen, Systeme zur Angriffserkennung einzusetzen, auch analog für Betreiber von Energieversorgungsnetzen und solchen Energieanlagen, die durch Inkrafttreten der Rechtsverordnung gemäß § 10 Absatz 1 BSIG als Kritische Infrastruktur bestimmt wurden, eingeführt.

Einschätzung:

Es wird auf die Einschätzung zu § 8a Absätze 1a und 1b verwiesen.

BDEW-Petitum:

Es wird auf das BDEW-Petitum zu § 8a Absätze 1a und 1b verwiesen.

Ansprechpartner

Yassin Bendjebbour
Betriebswirtschaft | Steuern | Digitalisierung
Telefon: +49 30 300199-1529
yassin.bendjebbour@bdew.de

Dr. Michaela Schmitz
Wasser und Abwasser
Telefon: +49 30 300199-1200
michaela.schmitz@bdew.de

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
19(4)759

Positionspapier zum IT-Sicherheitsgesetz 2.0

Das geplante IT-Sicherheitskennzeichen muss auf internationalen und Europäischen Normen und Standards basieren.

Dezember 2020

- Keine Parallelstrukturen aufbauen: Unsere Qualitätsinfrastruktur ist effizient und Grundlage für wirtschaftlichen Erfolg.
- Europäisch und international denken: Der Weg zu europäischen und internationalen Standards und Märkten führt über DIN und DKE.
- Standortvorteil nutzen: DIN und DKE sind Marktführer für IT-Sicherheits-Standardisierung.

DIN e. V.

Saatwinkler Damm 42/43
13627 Berlin
www.din.de

Kontakt:

Katja Krüger
Senior Government Relations Manager
Tel.: 030 2601-2439
E-Mail: katja.krueger@din.de

DKE

Stresemannallee 15
60596 Frankfurt
Germany
www.dke.de

Kontakt:

Johannes Koch
Leiter Nat. Normungspolitik
Tel.: 069 6308-268
E-Mail: johannes.koch@vde.com

Sichere und geschützte IT-Systeme sind zu einem wesentlichen Erfolgsfaktor der Digitalwirtschaft geworden. Wenn im Rahmen der digitalen Transformation immer mehr Internet of Things (IoT)-fähige Geräte in Unternehmen und Privathaushalten Einzug halten, rücken auch Fragen nach Produktsicherheit und -qualität sowie Verbraucherschutz vermehrt in den Fokus. DIN und DKE begrüßen vor diesem Hintergrund den Ansatz des geplanten IT-Sicherheitsgesetz 2.0 (IT-SiG 2.0) zur Stärkung der IT-Sicherheit in Deutschland. Mit dem darin vorgesehenen freiwilligen IT-Sicherheitskennzeichen sollen Risikobewusstsein und Beurteilungsfähigkeit von Verbrauchern gefördert werden. DIN und DKE, die nationalen Normungsorganisationen, kritisieren allerdings die in der Umsetzung des Kennzeichens vorgesehene Prozess- und Kompetenzverteilung nachdrücklich. Ein paralleles System zur Erarbeitung des Standes der Technik, einschließlich Konformitätsbewertung und Zertifizierung kann nicht im Interesse der staatlichen Regelsetzung sein, da es zu einer Zersplitterung der IT-Sicherheitsmarktes führen kann. Der Gesetzgeber sollte daher unbedingt auf bewährte Strukturen und die öffentlich-private Partnerschaft mit der deutschen Normung und weiteren Institutionen der nationalen Qualitätsinfrastruktur zurückgreifen.

Eine funktionierende Qualitätsinfrastruktur ist Grundlage für wirtschaftlichen Erfolg.

In Deutschland und Europa arbeiten Normung, Messwesen, Prüfdienstleister, Akkreditierung und Zertifizierung im Rahmen einer konsistenten Qualitätsinfrastruktur Hand in Hand, um die Sicherheit von Produkten und den Schutz von Verbrauchern sicherzustellen. Dieses System mit seinen spezifischen Zuständigkeiten hat sich seit Jahrzehnten bewährt.

- Eine effiziente Qualitätsinfrastruktur stellt die Einhaltung hoher Anforderungen an die Sicherheit und Qualität von Produkten und Dienstleistungen sicher.
- Der aktuelle Referentenentwurf zum IT-SiG 2.0 sieht vor, Kompetenzen, die bisher der Normung zugehörig sind, zunehmend beim Bundesamt für Sicherheit in der Informationstechnik (BSI) zu zentralisieren und damit ein paralleles System zur nationalen Qualitätsinfrastruktur aufzubauen[1]. Ein solches Parallelsystem zur Erstellung von technischen Richtlinien, Prüfverfahren und Konformitätsbewertungsprogrammen schafft unnötige Bürokratie, doppelte und längere Verfahren, zusätzliche Kosten und verschenkt das Potenzial für Synergien.
- Bei der Umsetzung des freiwilligen IT-Sicherheitskennzeichens sollte unbedingt auf die bewährten Prozesse der nationalen Qualitätsinfrastruktur zurückgegriffen werden, indem dem Kennzeichen insbesondere Europäische und internationale Normen und Standards zugrunde gelegt werden.

[1] z. B. in § 8a Abs. 1a BSIG-E: Demnach wird die Einhaltung des Stands der Technik für die Betreiber von Kritischen Infrastrukturen dann vermutet, wenn die getroffenen Maßnahmen einer Technischen Richtlinie (TR) des BSI in der jeweils geltenden Fassung entsprechen. Dies ist nicht nur im Hinblick auf das paritätisch ausgestaltete, nationale Normungsverfahren problematisch, sondern auch für die Schaffung von international und allgemein anerkannten Normen und Standards durch die Normenorganisationen ISO/IEC und CEN/CENELEC.

Durch kohärente internationale Normen haben deutsche Unternehmen Zugang zu Weltmärkten und gestalten diese mit. Der Weg zu europäischen und internationalen Standards führt über DIN und DKE.

Mit dem Normenvertrag von 1975 hat die Bundesrepublik Deutschland DIN als nationale Normungsorganisation und Vertreter Deutschlands in der europäischen und internationalen Normung anerkannt. Die Deutsche Normungsstrategie (2016) bekräftigt den Auftrag an DIN und DKE, als führende Moderationsplattformen Normungs- und Standardisierungsprozesse über die Grenzen der jeweils eigenen Organisation hinweg, auch für Foren und Konsortien, zu koordinieren. Gleichzeitig wird sichergestellt, dass das deutsche Normenwerk, bestehend aus internationalen, Europäischen und nationalen Normen, in sich kohärent und widerspruchsfrei ist. Die deutsche Wirtschaft baut auf dieses einheitliche Normenwerk, das ihr den Zugang zu Weltmärkten deutlich und nachhaltig erleichtert.

- Nationale technische Richtlinien, die außerhalb des bestehenden Normungs- und Standardisierungssystems erstellt werden, schaffen zusätzlichen Orientierungs- und Erfüllungsaufwand für Hersteller, Anwender und Verbraucher, führen zu höheren Kosten, begünstigen den Aufbau nicht-tarifärer Handelshemmnisse und wirken sich nachteilig auf die heimische Wirtschaft aus, da ihre Inhalte konträr zu europäischen und internationalen Normen und Standards sein können Die dadurch entstehenden Barrieren wirken einer europäischen Harmonisierung bei der Entwicklung von IT-Sicherheitsstandards im gemeinsamen europäischen Binnenmarkt entgegen.
- DIN und DKE bieten dem BSI zur Formulierung technischer Richtlinien den engen Schulterschluss an, um soweit möglich internationale bzw. europäische Lösungen anzustreben. Über DIN und DKE können Mitarbeiter des BSI die Erarbeitung kohärenter Normen und Standards anstoßen und in europäischen und internationalen Standardisierungsgremien mitwirken.

Marktführerschaft in der Standardisierung für IT-Sicherheit.

Im Bereich IT-Sicherheit hält Deutschland über DIN und DKE mit der Führung zentraler europäischer[2] und internationaler[3] Arbeitsgremien die Marktführerschaft in der IT-Sicherheits-Standardisierung – ein Standortvorteil, den es zu nutzen gilt. In diesen Gremien werden grundlegende Normen zur IT-Sicherheit gepflegt, beispielsweise die *DIN EN ISO/IEC 27000-Normenreihe für „Informationssicherheit-Managementsysteme“*, die *ISO/IEC 15408 „Evaluationskriterien für IT-Sicherheit"* oder die *Normenreihe IEC 62443 „Industrielle Kommunikationsnetze - IT-Sicherheit für Netze und Systeme“.* Diese internationalen Normen werden von deutschen Unternehmen erfolgreich angewendet. Die Konsolidierung der nationalen Meinung erfolgt im DIN-Normenausschuss Informationstechnik und Anwendungen (NIA) und im DKE-Normungskomitee „IT-Sicherheit in der Automatisierungstechnik“.

- Die konstruktive Zusammenarbeit zwischen BSI, Wirtschaft, Wissenschaft und Forschung in bestehenden und künftigen Normungsgremien sollte fortgesetzt und ausgebaut werden.

[2] CEN/CENELEC JTC 13 „Cybersecurity and Data Protection“
[3] ISO/IEC JTC1/SC 27 „Information Security, Cybersecurity and Privacy Protection“; IEC/TC 65/WG 10 “Security for industrial process measurement and control - Network and system security”

- Ein Beispiel, wie dies gelingen kann, ist die Erarbeitung der *DIN SPEC 27072 „IoT-fähige Geräte - Mindestanforderungen zur Informationssicherheit“*[4]. Der Standard richtet sich vor allem an Hersteller, Entwickler und Beschaffer entsprechender Produkte und kann als Grundlage zur Ausgestaltung des geplanten IT-Sicherheitskennzeichens genutzt werden.
- Ein weiteres Beispiel ist der Branchenspezifische Sicherheitsstandard (B3S) für Verkehrssteuerungs- und Leitsysteme im kommunalen Straßenverkehr (DIN VDE V 0832-700), der durch das BSI anerkannt wurde.
- Über DIN und DKE besteht die Möglichkeit, diese und ähnliche Inhalte in die europäische und internationale Normung einzubringen.

Ziel des IT-Sicherheitsgesetzes 2.0 ist ein ausreichendes Schutz- und Sicherheitsniveau, insbesondere für Verbraucher. Dieses Ziel kann aus den dargelegten Gründen bestmöglich erreicht werden, wenn dem einzuführenden IT-Sicherheitskennzeichen internationale und Europäische Normen zugrunde gelegt werden, an deren Erarbeitung und Pflege sich deutsche Stakeholder sowie die öffentliche Hand, z. B. vertreten durch das BSI, über die nationalen Normungsorganisationen DIN und DKE aktiv beteiligen. Ergänzt werden können diese Normen durch Standards, die mit dem deutschen Normenwerk kohärent sind (z. B. DIN SPEC 27072). Dadurch beugt der Gesetzgeber einer Fragmentierung der Standardisierungslandschaft und der digitalen Märkte vor, schafft praxistaugliche Regeln für Hersteller, Anwender, Beschaffer und Verbraucher und stellt sicher, dass die geschaffenen Lösungen europäisch skalierbar sind.

Wir empfehlen daher folgende inhaltliche Ergänzungen zum Diskussionsentwurf des Bundesministeriums des Innern, für Bau und Heimat vom 01.12.2020:

- Zu § 3 Abs. 1 Satz 2 Nr. 20 BSIG-E (S. 7 im Referentenentwurf): „Weiterentwicklung des Standes der Technik bei sicherheitstechnischen Anforderungen an IT-Produkte unter Berücksichtigung von bestehenden, insbesondere internationalen und europäischen, Normen und Standards.“
- Zu § 9c Abs. 3 Nr. 3 BSIG-E (S. 23 im Referentenentwurf): „Die IT-Sicherheitsanforderungen, auf die sich die Herstellererklärung bezieht, ergeben sich aus vom Bundesamt für die Anwendung als geeignet befundenen internationalen, europäischen und nationalen Normen und Standards, die den Stand der Technik abbilden. Liegt für einen Anwendungsbereich keine solche Norm oder kein solcher Standard vor kann das Bundesamt ein solches Projekt bei den nationalen Normungsorganisationen initiieren oder eine Technische Richtlinie erarbeiten, die den jeweiligen Anwendungsbereich umfasst und soweit möglich auf bestehende Normen oder Teile davon verweist. Wird ein Anwendungsbereich von mehr als einer Technischen Richtlinie umfasst, richten sich die Anforderungen nach der jeweils spezielleren Technischen Richtlinie. Liegt für die jeweilige Produktkategorie keine Technische Richtlinie vor, ergeben sich die IT-Sicherheitsanforderungen aus branchenabgestimmten IT-Sicherheitsvorgaben, sofern das Bundesamt festgestellt hat, dass diese Vorgaben geeignet sind, ausreichende IT-Sicherheitsanforderungen für die Produktkategorie abzubilden. Ein Anspruch auf diese

[4] Das Dokument wurde unter Beteiligung des BSI erarbeitet. Es enthält IT-Sicherheitsanforderungen und Empfehlungen für internetfähige Geräte im privaten oder kleingewerblichen Endkundenbereich wie z. B. IP-Kameras, Smart-TVs oder Smart Speaker.

Feststellung besteht nicht. Technische Richtlinien des Bundesamtes sollen stets Widerspruchsfreiheit mit internationalen, europäischen und nationalen Normen und Standards anstreben. Die Dauer, für die der Hersteller oder Diensteanbieter die Erfüllung der IT-Sicherheitsanforderungen zusichert, wird durch Rechtsverordnung nach § 10 Absatz 3 geregelt. Die Rechtsverordnung kann vorsehen, dass die für die jeweilige Produktkategorie maßgebliche Technische Richtlinie oder die branchenabgestimmten IT-Sicherheitsvorgaben eine abweichende Dauer festlegen können."

Über DIN

Das Deutsche Institut für Normung e. V. (DIN) ist die unabhängige Plattform für Normung und Standardisierung in Deutschland und weltweit. Als Partner von Wirtschaft, Forschung und Gesellschaft trägt DIN wesentlich dazu bei, die Marktfähigkeit von innovativen Lösungen durch Standardisierung zu unterstützen – sei es in Themenfeldern rund um die Digitalisierung von Wirtschaft und Gesellschaft oder im Rahmen von Forschungsprojekten. Rund 34.500 Experten aus Wirtschaft und Forschung, von Verbraucherseite und der öffentlichen Hand bringen ihr Fachwissen in den Normungsprozess ein, den DIN als privatwirtschaftlich organisierter Projektmanager steuert. Die Ergebnisse sind marktgerechte Normen und Standards, die den weltweiten Handel fordern und der Rationalisierung, der Qualitätssicherung, dem Schutz der Gesellschaft und Umwelt sowie der Sicherheit und Verständigung dienen. Weitere Informationen unter www.din.de.

Über DKE

Die DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE ist die in Deutschland zuständige Organisation für die Erarbeitung von Standards, Normen und Sicherheitsbestimmungen in den Themenfeldern Elektrotechnik, Elektronik und Informationstechnik. Als deutsches Mitglied in den internationalen und europäischen Organisationen für die Normung der Elektro- und Telekommunikationstechnik – IEC, CENELEC und ETSI – vertritt die DKE die deutschen Interessen bei der Erarbeitung und Weiterentwicklung der Internationalen und Europäischen Normen zum Abbau von Handelshemmnissen und zur weltweiten Öffnung der Märkte.