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.