Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
19(4)741 B

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

Stiftung Neue Verantwortung

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)

Stiftung Neue Verantwortung

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]