IT-SICHERHEIT IM VERBRAUCHERALLTAG STÄRKEN

Stellungnahme zum Entwurf eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (Zweites IT-Sicherheitsgesetz – IT-SiG 2.0) in der Fassung vom 16. Dezember 2020

7. Januar 2021

Impressum

Verbraucherzentrale
Bundesverband e.V.

Team
Digitales und Medien

Rudi-Dutschke-Straße 17
10969 Berlin
digitales@vzbv.de

Bundesverband der Verbraucherzentralen und Verbraucherverbände

Verbraucherzentrale Bundesverband e.V.

INHALT

I. ZUSAMMENFASSUNG

Der Verbraucherzentrale Bundesverband (vzbv) begrüßt, dass der Aufgabenbereich des Bundesamtes für Sicherheit in der Informationstechnik (BSI) um Verbrauchschutz und Verbraucherinformation erweitert wird. Dies kann zu einer verbesserten Marktüberwachung und Marktregulierung führen und die IT-Sicherheitslage aus Verbrauchersicht verbessern. Damit diese Ziele erreicht werden können, besteht jedoch noch nachstehend zusammengefasster Verbesserungsbedarf an dem vorliegenden Entwurf:

- Die Verankerung des Verbraucherschutzes und der Verbraucherinformation im Bereich der Sicherheit in der Informationstechnik als neue Aufgabe des BSI im BSI-Gesetz (BSIG-E) ist begrüßenswert. Bei der konkreten Ausgestaltung von Beratungs- und Informationsangeboten sollte darauf geachtet werden, Synergieeffekte zu bestehenden Angeboten von Verbraucherschutzorganisationen und anderen zivilgesellschaftlichen Akteuren herzustellen.
- Die Freigabe des IT-Sicherheitskennzeichens durch das BSI darf nicht auf einer Herstellererklärung beruhen. Vielmehr sollte das Kennzeichen vom BSI nur nach gründlicher technischer Prüfung vergeben werden.
- Die Bundesregierung muss sich auf europäischer Ebene für einen horizontalen Rechtsrahmen einsetzen, welcher verbindliche Sicherheitsanforderungen an Produkte (vernetzte Geräte und digitale Dienste) definiert.
- Es muss sichergestellt werden, dass die zukünftige Aufgabe des BSI im Bereich des Verbraucherschutzes nicht mit den übrigen Aufgabenbereichen des BSI, etwa der Unterstützung bei der Strafverfolgung, in Interessenskonflikte gerät.
- Bei der Bereinigung infizierter Nutzersysteme sollte auf unfreiwillige Eingriffe von außen verzichtet werden. Angemessene und verhältnismäßige Maßnahmen sollten unter Mithilfe aller betroffenen Telekommunikationsanbieter ohne Berücksichtigung ihrer Größe sowie ihrer technischen und wirtschaftlichen Möglichkeiten durchgeführt werden.

II. EINLEITUNG

Die Bundesregierung hat am 16. Dezember 2020 einen Entwurf zum geplanten Zweiten IT-Sicherheitsgesetz (IT-SiG-E)[1] beschlossen. Der vzbv hat sich bereits zu einem früheren Referentenentwurf geäußert[2]. Die nachfolgende Stellungnahme stellt eine Anpassung an die seitdem vorgenommenen Entwurfsänderungen dar und nimmt weitergehende Erkenntnisse zu den geplanten Neuregelungen auf.

Schwerpunkt des Entwurfs ist unter anderem eine umfassende Erweiterung von Aufgabenbereichen und Kompetenzen des BSI durch Änderungen des BSIG-E. So sollen Verbraucherschutz und Verbraucherinformation im Bereich der Sicherheit in der Informationstechnik zusätzliche Aufgaben des BSI werden (§ 3 Abs. 1 S. 2 Nr. 14a BSIG-

[1] Bundesministerium des Innern, für Bau und Heimat (16.12.2020): Kabinett beschließt Entwurf für IT-Sicherheitsgesetz 2.0 (Zweites IT-Sicherheitsgesetz – IT-SiG 2.0), https://www.bmi.bund.de/SharedDocs/pressemitteilungen/DE/2020/12/it-sig-2-kabinett.html, 04.01.2021.

[2] Verbraucherzentrale Bundesverband e.V. (2020): IT-Sicherheit im Verbraucheralltag stärken, https://www.vzbv.de/dokument/it-sicherheit-im-verbraucheralltag-staerken, 04.01.2021.

E). Außerdem soll ein freiwilliges IT-Sicherheitskennzeichen für Produkte eingeführt werden (§ 9c BSIG-E).

III. DIE FORDERUNGEN IM EINZELNEN

1. AUFGABENBEREICH VERBRAUCHERSCHUTZ

Während der Aufgabenschwerpunkt des BSI nach dem aktuell geltenden BSIG noch auf dem Schutz kritischer Infrastrukturen und der Informationstechnik (IT) des Bundes liegt, soll das BSI gemäß § 3 Abs. 1 S. 2 Nr. 14a BSIG-E nun zusätzliche Aufgaben im Bereich des Verbraucherschutzes und der Verbraucherinformation wahrnehmen.

Tatsächlich stellt es für Verbraucherinnen und Verbraucher[3] einen großen Mehrwert dar, zusätzlich von technisch kompetenter staatlicher Stelle Beratungen, Informationen und Warnungen zu erhalten. Bedeutende Sicherheitslücken wurden in der Vergangenheit häufig von Sicherheitsforschern oder zivilgesellschaftlichen Organisationen, und nicht von zuständigen staatlichen Stellen entdeckt und publiziert. So war es der norwegische Verbraucherschutzverband Forbrukerrådet, der auf IT-Sicherheitsprobleme beim Smart-Toy „Cayla“ aufmerksam machte[4].

Daher ist es zu begrüßen, wenn nun die Überwachung des Marktes systematischer als bisher erfolgt und das BSI seine technischen Ressourcen zur sicherheitstechnischen Untersuchung von Produkten einsetzt, wie in der Begründung des Entwurfs vorgeschlagen. Ebenfalls zu begrüßen ist das Vorhaben, dass das BSI „mit den Verbraucherorganisationen und weiteren Partnern im Bereich des (digitalen) Verbraucherschutzes eng zusammenarbeiten“ solle[5]. Aus Verbrauchersicht ist relevant, dass sich das BSI mit tiefergehenden technischen Informationen und Prüfungen in den digitalen Verbraucherschutz einbringt und so zivilgesellschaftliche Akteure wie beispielsweise die Stiftung Warentest, die Verbraucherzentralen und die Marktbeobachtung Digitales des vzbv in ihrer Arbeit sinnvoll ergänzt. Insbesondere bei der Ausgestaltung der geplanten „Verbraucherschutz-Online-Plattform“[6] und anderer Informationsportale sollten Überschneidungen zu bereits bestehenden Informations- und Beratungsangeboten der Verbraucherzentralen[7] und anderer Akteure vermieden und Synergieeffekte genutzt werden.

> Der vzbv begrüßt die Verankerung des Verbraucherschutzes und der Verbraucherinformation im Bereich der Sicherheit in der Informationstechnik als neue Aufgabe des BSI im BSI-Gesetz. Bei der konkreten Ausgestaltung dieser Aufgabe sollten vertiefte technische Tests und Konformitätsbewertungen, die Information über Produkt- und Technologierisiken sowie technische Beratungsleistungen und Warnmeldungen im Vordergrund stehen. Des Weiteren sollte insbesondere bei der Ausgestaltung

[3] Die im weiteren Text gewählte männliche Form bezieht sich immer zugleich auf Personen aller Geschlechter. Wir bitten um Verständnis für den weitergehenden Verzicht auf Mehrfachbezeichnungen zugunsten einer besseren Lesbarkeit des Textes.

[4] Forbrukerrådet (2016): Connected toys violate European consumer law: https://www.forbrukerradet.no/siste-nytt/connected-toys-violate-consumer-laws/, 24.11.2020.

[5] IT-SiG-E, S. 68 f.

[6] Ebd., S. 69.

[7] Bsp. Verbraucherzentrale NRW e.V. (2020): „Digitale Welt“, https://www.verbraucherzentrale.de/wissen/digitale-welt, 03.12.2020.

von Beratungs- und Informationsangeboten darauf geachtet werden, Synergieeffekte zu bestehenden Angeboten von Verbraucherschutzorganisationen und anderen zivilgesellschaftlichen Akteuren herzustellen.

2. FREIWILLIGES IT-SICHERHEITSKENNZEICHEN

Aufgrund der technischen Komplexität und weil IT-Sicherheit wegen aktueller Bedrohungsszenarien eine sehr dynamische Größe ist, können Verbraucher das Sicherheitsniveau eines Produktes in der Regel nicht eigenständig beurteilen. Daher ist es wichtig, dass sie bei der Kaufentscheidung verlässliche Informationen über das Sicherheitsniveau eines Produktes zum Zeitpunkt des Erwerbs und über den gesamten Produktlebenszyklus erhalten.

Der vzbv bevorzugt in diesem Zusammenhang verbindliche gesetzliche Regelungen zu Sicherheitsanforderungen von Produkten gegenüber freiwilligen Kennzeichnungen.

2.1 Europäischer Rechtsrahmen für vernetzte Geräte und digitale Dienste

Das BSIG-E sieht allein für kritische Infrastrukturen und für die IT des Bundes umfassende verpflichtende Sicherheitsanforderungen mit entsprechenden Kontrollbefugnissen für das BSI vor. Für den Bereich der Verbraucherprodukte werden im BSIG-E hingegen lediglich technisch-organisatorische Maßnahmen auf Seiten der Betreiber digitaler Dienste gefordert (§ 8c BSIG-E). Diese Regeln sind im Zuge der Umsetzung der europäischen Richtlinie zur Netz- und Informationssicherheit (NIS-Richtlinie) erlassen und daher im aktuellen Entwurf nicht angepasst worden. Sie beziehen sich schwerpunktmäßig auf das Prozessmanagement von Diensteanbietern, weniger auf konkrete technische Produkteigenschaften.

Aus Verbrauchersicht ist es jedoch insbesondere im Hinblick auf vernetzte Geräte im Internet der Dinge erforderlich, technisch konkrete und verpflichtende Sicherheitsanforderungen zu definieren (Security by Design, Security by Default). Verbraucher müssen darauf vertrauen können, dass ein Produkt zum Zeitpunkt des Erwerbs und während des gesamten Lebenszyklus ein angemessenes Sicherheitsniveau bietet. Diese Anforderungen sollten in einem horizontalen europäischen Regulierungsrahmen geregelt werden.

Der vzbv hat in einem Positionspapier anlässlich der Konsultation der Europäischen Kommission zur Reform der NIS-Richtlinie die aus Verbrauchersicht erforderlichen verpflichtenden Sicherheitsanforderungen bei vernetzten Geräten dargelegt[8]. Auch wenn das Zweite IT-Sicherheitsgesetz nicht den geeigneten regulatorischen Ansatzpunkt bietet, sollte die Bundesregierung das Ziel, einen europäischen Rahmen für verpflichtende gesetzliche Sicherheitsanforderungen für Produkte zu schaffen, klar benennen. Der vzbv begrüßt in diesem Zusammenhang die jüngst veröffentlichten Schlussfolgerungen des Rates der Europäischen Union zur Cybersicherheit vernetzter Geräte[9].

---

[8] Verbraucherzentrale Bundesverband e.V. (2020): Digitale Dienste und Geräte sicher gestalten, https://www.vzbv.de/dokument/digitale-dienste-und-geraete-sicher-gestalten, 04.12.2020.

[9] The Council of the European Union (2020): Council Conclusions on the cybersecurity of connected devices, https://data.consilium.europa.eu/doc/document/ST-13629-2020-INIT/en/pdf, 04.12.2020.

2.2 Anforderungen und Freigabeverfahren des IT-Sicherheitskennzeichens

§ 9c BSIG-E sieht ein freiwilliges IT-Sicherheitskennzeichen mit dem Ziel vor, informierte Entscheidungen zum Erwerb von Produkten hinsichtlich ihres IT-Sicherheitsniveaus zu ermöglichen. Damit ein solches Kennzeichen aber tatsächlich ein geeignetes Unterscheidungskriterium für IT-Sicherheit sein kann, muss die dadurch getroffene Sicherheitsaussage verlässlich sein und über die gesamte Produktlebensdauer hinweg aktuell bleiben. Leider stellt § 9c BSIG-E diesbezüglich deutlich zu geringe Anforderungen an eine Freigabe des Kennzeichens durch das BSI. Diese bestehen aus einer Herstellererklärung und einer Plausibilitätsprüfung einzureichender technischer Unterlagen (§ 9c Abs. 5 BSIG-E). Eigene Prüfungen durch das BSI oder qualifizierte Prüfstellen wie bei der Zertifizierung nach Technischen Richtlinien des BSI[10] sind hingegen optional und scheinen lediglich für den Zeitraum nach Erteilung des Kennzeichens vorgesehen zu sein (§ 9c Abs. 8 BSIG-E). Auf das System der Vertrauenswürdigkeitsstufen der europäischen Schemata für die Cybersicherheitszertifizierung im EU-Rechtsakt zur Cybersicherheit[11] (Art. 52) übertragen, befindet sich das deutsche IT-Sicherheitskennzeichen damit auf der Vertrauenswürdigkeitsstufe „niedrig“. Wie der Entwurf in der Begründung selbst deutlich macht, hat das Kennzeichen deshalb nicht die Qualität des eigentlich im Koalitionsvertrag angekündigten „Gütesiegels für IT-Sicherheit“[12]. Denn hierzu wären Prüfungen durch unabhängige Stellen erforderlich[13].

Aus Verbrauchersicht muss dieser Unterschied auf dem Kennzeichen optisch deutlich gemacht werden. In der grafischen Umsetzung des Kennzeichens darf nicht allein das BSI als Freigabeinstanz im Mittelpunkt stehen. Das Kennzeichen muss auch explizit angeben, wenn es aufgrund einer Herstellererklärung vergeben wurde. Falls technische Prüfungen vor der Freigabe stattgefunden haben, so sollte dies ebenfalls vermerkt werden. Dadurch entstünde eine abgestufte Kennzeichnung, die dem Verbraucher schnell und direkt den Vergleich verschiedener mit dem Kennzeichen versehener Produkte ermöglichen würde. Es muss in der nach § 10 Abs. 3 vorgesehenen Rechtsverordnung näher bestimmt werden, dass diese Informationen direkt auf dem Kennzeichen angebracht und nicht lediglich verlinkt werden. Insgesamt sollte aber auf die Möglichkeit einer Herstellererklärung zugunsten einer vertieften technischen Prüfung vor Freigabe des Kennzeichens verzichtet werden.

Auch im Hinblick auf die technischen Bewertungsmaßstäbe bestehen problematische Unwägbarkeiten. Zwar sollte das Kennzeichen auf der Grundlage der vom BSI erlassenen Technischen Richtlinien vergeben werden. Jedoch wird die Möglichkeit offengelassen, dass für eine zu kennzeichnende Produktgruppe noch keine entsprechende Richtlinie erlassen wurde und stattdessen „branchenabgestimmte IT-Sicherheitsvorgaben“ maßgeblich sein können (§ 9c Abs. 3 BSIG-E). In diesen Fällen bestünde die Gefahr, dass Vorgaben zu sehr den Interessen der Hersteller und Anbieter entsprechen. Dieser Umstand ist besonders brisant, da die Erstellung Technischer Richtlinien zeitaufwendig

[10] BSI (2020): Zertifizierung nach Technischen Richtlinien, https://www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/Produktzertifizierung/ZertifizierungnachTR/zertifiz_tr.html, 04.12.2020.

[11] Verordnung (EU/2019/881) vom 17. April 2019 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik und zur Aufhebung der Verordnung (EU) Nr. 526/2013 (Rechtsakt zur Cybersicherheit).

[12] Ein neuer Aufbruch für Europa. Eine neue Dynamik für Deutschland. Ein neuer Zusammenhalt für unser Land. Koalitionsvertrag zwischen CDU, CSU und SPD.19. Legislaturperiode (2018). https://www.bundesregierung.de/breg-de/themen/koalitionsvertrag-zwischen-cdu-csu-und-spd-195906, 2.12.2020. Z. 1988 ff.

[13] IT-SiG-E, S. 101 f.

ist und in absehbarer Zeit daher die Branchenvorgaben möglicherweise vorrangig als Freigabegrundlage für das Kennzeichen herangezogen werden müssten. Daher wäre es besser, auf die Heranziehung branchenabgestimmter Vorgaben zu verzichten.

Die Modalitäten der Freigabe bleiben also im Gesetzesentwurf weit hinter den Prüfmöglichkeiten zurück, die die Vergabe von Zertifizierungen gemäß Technischer Richtlinien im BSI aktuell bietet. Es besteht daher die Gefahr einer Scheinsicherheit durch ein Kennzeichen, dessen Sicherheitsversprechen auf industriefreundlichen Normen und ungeprüften Herstellererklärungen fußt. Ungenügend ist auch die Regelung zum Erhalt eines bestätigten Sicherheitsniveaus durch Updates. Zwar soll der Zeitraum, in dem Sicherheitsupdates geliefert werden müssen, durch das Kennzeichen definiert werden (§ 9c Abs. 3 BSIG-E). Jedoch ist weder verbindlich geregelt, ob die Erfüllung dieser Pflicht über die gesamte Geltungszeit des Kennzeichens hinweg überprüft wird, noch, wie der Käufer gegebenenfalls vom Erlöschen beziehungsweise dem Widerruf der Freigabe für das Kennzeichen erfährt.

Falls ein Produkt vor Ablauf der im Kennzeichen festgelegten Frist durch ausbleibende Updates unsicher wird, kann das BSI zwar die Freigabe des Kennzeichens widerrufen (§ 9c Abs. 8 S. 2 Nr. 2 BSIG-E), und eine entsprechende Information kann über einen mit dem Kennzeichen verbundenen Link beziehungsweise QR-Code[14] erfolgen. Da eine solche Verlinkung aber sicher im Nutzungsalltag nicht ständig aufgerufen wird, wäre die Gefahr gegeben, dass der Verbraucher das unsichere Produkt über längere Zeit nichtsahnend weiternutzt.

Der Entwurf legt in diesem Zusammenhang leider keine geeigneten Informationskanäle zu den Verbrauchern fest. Dieser Fall könnte vermieden werden, indem die geforderte Updatedauer deutlich auf dem Kennzeichen selbst erwähnt wird. Es ist auch nicht zu akzeptieren, dass die Zeitdauer durch eine ministeriale Rechtsverordnung, bei deren Erlass ausschließlich Wirtschaftsverbände konsultiert werden, bestimmt werden soll (§ 9c Abs. 3 BSIG-E).

- Die Freigabe des IT-Sicherheitskennzeichens durch das BSI darf nicht auf einer Herstellerklärung beruhen. Sie muss dem Verfahren für die Zertifizierungen nach Technischen Richtlinien des BSI vollumfänglich entsprechen und unabhängige Prüfungen umfassen, die beispielsweise auch die laufende Bereitstellung von Updates nach Inverkehrbringung mit einbeziehen.
- Freigabekriterien, Freigabeart (Herstellererklärung) und Gültigkeitsdauer müssen auch auf dem Kennzeichen selbst deutlich angegeben werden.
- Die Bundesregierung muss sich auf europäischer Ebene für einen horizontalen Rechtsrahmen einsetzen, welcher verbindliche Sicherheitsanforderungen an Produkte (vernetzte Geräte und digitale Dienste) definiert.

3. DAS VERHÄLTNIS VON VERBRAUCHERSCHUTZ UND ÖFFENTLICHER SICHERHEIT

Durch seine Rolle bei der Prüfung und Überwachung digitaler Dienste und Produkte erlangt das BSI in seiner Arbeit eine große Zahl von sicherheitsrelevanten Informationen, auch personenbezogene oder personenbeziehbare Daten von und über Verbraucher. Es gehört zur Arbeit des BSI im Bereich des Verbraucherschutzes, Nutzer frühzeitig

[14] IT-SiG-E, S. 101.

über aktuelle Sicherheitsgefahren zu informieren, diese sollen sich auch mit individuellen Sicherheitsproblemen an das Amt wenden können. Anbieter und Hersteller sollen beim Finden und Verhindern von Sicherheitsproblemen eng mit dem BSI zusammenarbeiten. Im aktuellen BSIG-E werden die entsprechenden Kompetenzen noch einmal ausgeweitet. So darf das BSI proaktiv Server-Schnittstellen im Internet auf Sicherheitslücken prüfen (§ 7b Abs. 1 BSIG-E) und von Telekommunikationsdienstleistern Bestandsdaten abfragen (§ 5c BSIG-E).

Diese mit dem neuen Entwurf noch wichtiger gewordene Rolle des BSI erfordert unbedingt, dass es das volle Vertrauen der Zivilgesellschaft und der Wirtschaft genießt. Eine wichtige Voraussetzung dafür ist, dass der digitale Verbraucherschutz sachbezogen und frei von Interessenskonflikten umgesetzt werden kann. Dies ist jedoch von zivilgesellschaftlichen und von wirtschaftsnahen Akteuren mit dem Hinweis auf die Aufsicht des Bundesministerium des Innern, für Bau und Heimat (BMI) über das BSI in Zweifel gezogen worden[15]. Konkrete Befürchtungen in diesem Zusammenhang sind beispielsweise, dass erkannte Sicherheitslücken nicht veröffentlicht werden könnten, um sie für offensive Zwecke der Strafverfolgung zu nutzen.

Diesen Unwägbarkeiten kann begegnet werden, indem die verschiedenen Aufgaben des BSI für den Verbraucherschutz einerseits und die Zuarbeit für andere Sicherheitsbehörden andererseits gesetzlich genauer umrissen werden. In diesem Zusammenhang sind insbesondere Überlegungen zu einem staatlichen „Schwachstellenmanagement“ zu erwähnen[16]. Der aktuelle Gesetzgebungsprozess ist eine Gelegenheit, das Nebeneinander der Fachaufsichten des BMI über Strafverfolgungsbehörden, Nachrichtendienste und das BSI zu thematisieren. Die Fachaufsicht könnte beispielsweise durch gesetzliche Regelungen ergänzt oder auf bestimmte Tätigkeitsbereiche des BSI begrenzt werden.

> Das Handeln des BSI im Bereich des digitalen Verbraucherschutzes muss frei von Zielkonflikten sein. Um dies sicherzustellen, könnte die Fachaufsicht des BMI durch gesetzliche Regelungen ergänzt oder auf bestimmte Tätigkeitsbereiche des BSI begrenzt werden.

4. SICHERHEITSANFORDERUNGEN AN TELEKOMMUNIKATIONSDIENSTE

Der neue § 7c des BSIG-E erteilt dem BSI bei Vorliegen „konkreter erheblicher“ Gefahren die Befugnis, Telekommunikationsanbietern technische Maßnahmen zur Beseitigung dieser Gefahren auferlegen zu können. Als Beispiel nennt der Entwurf in der Begründung ein Botnetz aus infizierten Endgeräten, die von einem Kontrollserver koordiniert und für Überlastungsangriffe[17] auf andere Systeme benutzt werden[18]. Zur Abwehr solcher Gefahren sieht der Entwurf die Anordnung von Maßnahmen vor, die bereits in § 109a Abs. 5 und 6 des Telekommunikationsgesetzes (TKG) vorgesehen sind und bis-

[15] Meister, Andre (2020): Seehofer will BSI zur Hackerbehörde ausbauen, https://netzpolitik.org/2020/seehofer-will-bsi-zur-hackerbehoerde-ausbauen/. Bitkom (2020): Bitkom fordert Nachbesserungen beim IT-Sicherheitsgesetz 2.0, https://www.bitkom.org/Presse/Presseinformation/Bitkom-fordert-Nachbesserungen-beim-IT-Sicherheitsgesetz-20, 24.11.2020. [Beide Stellungnahmen beziehen sich auf einen früheren Gesetzesentwurf].

[16] Dr. Herpig, Sven (2018): Schwachstellen-Management für mehr Sicherheit, https://www.stiftung-nv.de/de/publikation/schwachstellen-management-fuer-mehr-sicherheit, 04.01.2021.

[17] Sogenannte “Distributed Denial-of-Service”-Angriffe (DDoS).

[18] IT-SiG-E S. 83 ff.

lang im Ermessen der Telekommunikationsanbieter liegen. Sie beinhalten die Möglichkeit, dass Anbieter die durch sie kontrollierten Datenübertragungen umleiten, einschränken oder sogar unterbinden. Das kann für den Nutzer konkret heißen, dass sein Internetzugang gekappt wird und automatische Umleitungen von Netzwerkaufrufen stattfinden. Diese Regelung kann beispielsweise auf Router, die mit Schadsoftware infiziert sind, angewendet werden. Zwar haben Verbraucher ein eigenes Interesse daran, dass ihre Systeme nicht für kriminelle Zwecke missbraucht werden, und sie könnten durch Schadsoftware auf ihren Geräten auch direkt persönlichen Schaden erleiden. Jedoch sind diese Maßnahmen im Einzelnen auf Angemessenheit und Verhältnismäßigkeit zu prüfen, da sie die Nutzung netzbasierter Dienste durch Verbraucher deutlich einschränken.

Vor dem Hintergrund des in der Entwurfsbegründung geschilderten Szenarios eines DDoS-Angriffs erscheint ein „zeitnahes konzertiertes Vorgehen aller betroffenen Diensteanbieter“[19] im Rahmen der Anordnung durch das BSI plausibel. Es ist daher verhältnismäßig, dass die Durchführung von Schutzmaßnahmen nicht mehr allein im Ermessen der Diensteanbieter sein soll. Diesem Ziel steht aber entgegen, dass die Maßnahmen von der Größe des Anbieters und seinen technologischen und wirtschaftlichen Fähigkeiten abhängig gemacht werden (§ 7c Abs. 1 S. 1). Auf diese Weise kann die geforderte „bundesweit einheitliche IT-Sicherheit“[20] nicht gewährleistet werden. Die Einschränkung führt vielmehr zu systemischen Schwachstellen in den Telekommunikationsnetzen, denn wenn eine bestimmte Schadsoftware im Umlauf ist und das BSI Diensteanbieter darüber informiert, bleiben die Infrastrukturen der kleineren Anbieter gegenüber dieser Gefahr ungeschützt. Damit wären Kunden kleinerer Anbieter mit betroffenen Geräten gesetzlich schlechter gestellt als Kunden größerer Anbieter. Dies ist aus Verbrauchersicht nicht nachvollziehbar.

Zusätzlich zu den bereits in § 109a TKG verankerten Schutzmaßnahmen führt das BSIG-E eine neue Maßnahme ein, dass Telekommunikationsanbieter in Zusammenarbeit mit dem BSI per Fernzugriff infizierte Nutzersysteme bereinigen sollen (§ 7c Abs. 1 S. 1 Nr. 2). Diese Maßnahme stellt einen massiven Eingriff in Nutzersysteme dar und muss daher angemessen und verhältnismäßig sein. Dies ist jedoch nicht der Fall, denn bereits die Umleitung von Datenverkehr innerhalb der eigenen Netze der Telekommunikationsanbieter kann dazu verwendet werden, über eine Störung zu informieren und diese zu beseitigen. Auf diese Möglichkeit weist die Bundesnetzagentur in einer Handreichung auch explizit hin[21]. Nach einer Umleitung des Datenverkehrs innerhalb der eigenen Netze wäre eine Bereinigung des betroffenen Systems durch den Nutzer selbst möglich. Dieses Verfahren unter Mitwirkung des Nutzers ist einer behördlich angeordneten Bereinigung per Fernzugriff unbedingt vorzuziehen. Auf die in § 7c Abs. 1 S.1 Nr. 2 des BSIG-E genannte Maßnahme kann und sollte daher verzichtet werden.

---

[19] IT-SiG-E S. 84.

[20] Ebd., S. 83.

[21] Bundesnetzagentur (2020): Katalog von Sicherheitsanforderungen für das Betreiben von Telekommunikations- und Datenverarbeitungssystemen sowie für die Verarbeitung personenbezogener Daten nach § 109 Telekommunikationsgesetz (TKG). Version 2.0, https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Anbieterpflichten/OeffentlicheSicherheit/KatalogSicherheitsanforderungen/KatalogSicherheitsanforderungen2.pdf?__blob=publicationFile&v=3, 23.12.2020, S. 33.

Regelungen zu infizierten Nutzersystemen nach § 7c des BSIG-E sollten auf unfreiwillige Eingriffe in Nutzersysteme verzichten. Die in § 7c Abs. 1 S.1 Nr. 2 des BSIG-E genannte Maßnahme sollte daher entfallen.

Angemessene und verhältnismäßige Maßnahmen müssen unter Mithilfe aller betroffenen Telekommunikationsanbieter ohne Berücksichtigung ihrer Größe sowie ihrer technischen und wirtschaftlichen Möglichkeiten durchgeführt werden. Das BSI sollte Anbieter bei der Durchführung der Sicherheitsmaßnahmen bestmöglich technisch beraten und unterstützen.