Vorläufige Bewertung des Referentenentwurfs zum IT-Sicherheitsgesetz 2.0

Beitrag

Die folgende Bewertung basiert auf dem Gesetzesentwurf in der Version, die am 3. April 2019 durch Netzpolitik.org veröffentlicht wurde.[1]

Der erste Kritikpunkt an diesem Entwurf bezieht sich auf die Tatsache, dass die Aktualisierung des Gesetzes ohne eine vorhergehende Evaluierung des vorangegangenen Gesetzes geplant wurde. Das ist schwer nachvollziehbar. Schon bei dem Entwurf der Cybersicherheitsstrategie für Deutschland 2016 gab es keine Evaluierung der Cybersicherheitsstrategie 2011. Das wiegt in dem vorliegenden legislativen Vorhaben zum IT-Sicherheitsgesetz 2.0 noch weitaus schwerer, da im Vorgängergesetz sogar eine Teilevaluierung rechtlich verankert wurde (IT-Sicherheitsgesetz, Artikel 10)[2]. Die Evaluierung von Maßnahmen ist ein elementarer Bestandteil staatlichen Handelns und sollte vor allem bei diesem Gesetzgebungsvorhaben durchgeführt werden, bevor eine Kompetenz- und Anforderungsausweitung verabschiedet wird.

Die Regulierung von IT-Sicherheit ist ein komplexes Unterfangen. Es trägt wenig zu einer Vereinfachung und Versachlichung der Debatte bei, wenn das zuständige Bundesministerium des Innern, für Bau und Heimat neben den Maßnahmen zur Erhöhung der Sicherheit informationstechnischer Systeme auch Befugnisse für Sicherheitsbehörden unterbringt; vor allem solche, die nichts mit IT-Sicherheit zu tun haben.[3] Dies führt zur unnötigen Vermischung von öffentlicher Sicherheit und IT-Sicherheit und macht das legislative Vorhaben weniger transparent. Eine klare Trennung dieser beiden Bereiche und Unterbringung in separaten Gesetzgebungsvorhaben wäre angebracht.

Der aktuelle Gesetzesentwurf ignoriert weiterhin die im Koalitionsvertrag festgelegte "gleichzeitige und entsprechende Ausweitung der parlamentarischen Kontrolle" bei Ausweitung der Befugnisse der Sicherheitsbehörden[4]. Das ist höchst problematisch, da die Bundesregierung bisher noch immer nicht die vom Bundesverfassungsgericht angemahnte Gesamtschau der staatlichen Überwachungsmaßnahmen ("Überwachungsgesamtrechnung") [5] vorgelegt hat. Eine Befugniserweiterung der Sicherheitsbehörden im IT-Sicherheitsgesetz 2.0 muss deshalb durch geeignete und angemessene Schutzmechanismen und Kontrollmaßnahmen begrenzt werden.

Expertise bei Cyber- und Informationssicherheit ist nicht nur in den beteiligten Behörden und Verbänden zu finden. Daher wäre eine pre-legislative Einbindung der Zivilgesellschaft in den Strategie- und Gesetzgebungsprozess ein starkes Signal dafür, dass sich die Bundesregierung für eine gesamtgesellschaftliche Teilhabe einsetzt. Ein Vorhaben, das auch von der ehemaligen Bundesjustizministerin unterstützt wird.[6]

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"[7] wird in dem Entwurf nicht eingegangen. Der Entwurf sollte zumindest eine Prüfung unterschiedlicher Unabhängigkeitsmodelle (z.B. Statistisches Bundesamt oder Bundesbeauftragter für den Datenschutz und die Informationsfreiheit)[8] vorsehen.

Zu dem Mangel empirischer Evidenz bei der Normengestaltung und den genannten strategischen Defiziten kommen unklare oder zu weit gefasste Normen (s. Einzelkritik) sowie handwerkliche Fehler (u. a. Verweis auf nicht mehr aktuelle Norm, sprachliche Inkonsistenzen) hinzu. Eine Überarbeitung des Referentenentwurfs wäre daher zielführend um die Cyber- und Informationssicherheit in Deutschland nachhaltig zu stärken.

Einzelkritik zum IT-Sicherheitsgesetz 2.0 (nicht abschließend)

§ 2 Absatz 14 BSIG

Es ist unklar, in welchem Verhältnis die bisherigen "Institutionen im besonderen staatlichen Interesse" (INSI)[9] zu den neugeschaffenen "Infrastrukturen im besonderen öffentlichen Interesse" stehen. Weder in der EU NIS-Richtlinie[10] noch in dem entsprechenden Umsetzungsgesetz[11] finden sich diese Begrifflichkeiten wieder. Im Umsetzungsgesetz wird

lediglich einmal von "informationstechnischen Systemen von besonderem öffentlichen Interesse" gesprochen (BSIG § 5a Absatz 2). Diese Inkonsistenzen wirken einer Harmonisierung entgegen und verstärken unnötig die Komplexität durch die Einführung einer *KRITIS-Light* (gem. § 8f BSIG gelten auch für sie die KRITIS-Vorschriften aus §§ 8a und 8b BSIG).

Weiterhin ist nicht ersichtlich, warum "Kultur und Medien" als besonders schützenswert für das Gemeinwesen erachtet werden, nicht aber politische Parteien.[12] Zusätzlich handelt es sich bei Kultur und Medien um Bereiche in Zuständigkeit von Ländern und Kommunen.[13] Es ist unklar, ob eine entsprechende Konsultation der Länderebene stattgefunden hat.

§ 4b BSIG

Hier fehlt eine defensive Zweckbindung, damit Meldende sicher gehen können, dass die Informationen, vor allem zu Sicherheitslücken und Schadprogrammen, ausschließlich zur Erhöhung der IT-Sicherheit und nicht für offensive Zwecke eingesetzt werden.

§ 7a BSIG

Die Norm enthält keinerlei Einschränkung darüber, welche informationstechnischen Produkten und Systeme das Bundesamt für Sicherheit in der Informationstechnik untersuchen darf (Absatz 1). Darüber hinaus darf es auch noch alle Informationen darüber von den Herstellern einfordern (Absatz 2). Eine anlasslose Untersuchung aller informationstechnischen Systeme mit einer Befugnis, alle notwendigen Informationen anzufordern, ist sehr unspezifisch. Gleichzeitig werden dem Bundesamt kaum Beschränkungen auferlegt, wie es mit den so erworbenen Informationen verfahren darf (Verweis auf die sehr breite Norm BSIG §3 Absatz 1 Satz 2). Nach hiesiger Lesart beinhaltet dies auch die Weitergabe von erlangten Informationen zu Schwachstellen an andere Sicherheitsbehörden zur Erfüllung ihrer Aufgaben. An dieser Stelle sollte zumindest eine weitere defensive Zweckbindung der so erlangten Informationen über die Produkte und Systeme eingefügt werden (Absatz 2 und 3).

§ 8 Absatz 4 BSIG

Die Norm lässt “frühzeitig” undefiniert und verbessert die aktuelle Situation deswegen nicht, weil das Bundesamt für Sicherheit in der Informationstechnik immer noch gegenüber dem Bundesministerium des Innern, für Bau und Heimat fachlich weisungsgebunden ist und damit

die entsprechenden Anfragen anderer Stellen des Bundes theoretisch weiterhin über das Ministerium gehen müssen.

§ 8a Absatz 6 BSIG

Es handelt sich hierbei um eine *Carte Blanche* Formulierung, die dem Bundesministerium des Innern, für Bau und Heimat eine spätere Regulierung der Hersteller von KRITIS-Kernkomponenten über ihre gesamte Lieferkette einräumt, ohne irgendwelche weiteren Vorgaben für diese "Vertrauenswürdigkeitserklärung" zu machen. Die Auswirkungen und Konsequenzen einer solchen Regulierung durch eine Platzhalternorm sind unabsehbar.

§ 8g Absatz 2 BSIG

Mit Einführung einer "Cyberkritikalität" kann das Bundesamt für Sicherheit in der Informationstechnik die Pflichten gegenüber KRITIS-Unternehmen gem. §§ 8a und 8b BSIG auf Unternehmen ausdehnen, die weder KRITIS-Unternehmen gem. § 2 Absatz 10 BSIG, noch Infrastrukturen im besonderen öffentlichen Interesse gem. § 2 Absatz 14 BSIG sind.

§ 8h BSIG

Die Norm kann so gedeutet werden, dass die Übermittlungspflicht auch Informationen über Schwachstellen in IT-Produkten beinhaltet. Analog zu BSIG § 7a sollte auch hier eine defensive Zweckbindung der Informationsübermittlung integriert werden.

Weiterhin ist unklar, woher Hersteller von IT-Produkten wissen sollen, dass ihre Produkte in Institutionen gem. § 2 Absatz 10 und Absatz 14 BSIG (KRITIS und Infrastrukturen im besonderen öffentlichen Interesse) verbaut sind und daher zu erheblichen Störungen führen können. Grundlage ist lediglich, dass eine Beeinträchtigung dieser Anlagen zu "tatsächlichen und hinreichend schweren Gefährdung für ein Grundinteresse der Gesellschaft führen würde". Es ist unklar, welche Definition dem zugrunde liegt und der Abschnitt liest sich eher wie eine weitere *Carte Blanche* Regulierung.

§ 9a BSIG

Die gesetzliche Regelung von freiwilligen IT-Sicherheitskennzeichen lässt wenig Potenzial für mehr IT-Sicherheit erkennen, wird aber vermutlich eine große Anzahl an Ressourcen u. a. beim BSI beanspruchen. Fraglich ist, warum diese Norm nicht durch die Förderung bestehender Projekte (z.B. Trustable Technology Mark for the Internet of Things)[14] gefördert wird.

§ 109a Absatz 8 TKG

Es handelt sich hierbei um einen angeordneten Eingriff in das Computergrundrecht. Es ist unklar, wie die operative Umsetzung aussähe und welche Schutzmechanismen ergriffen werden, damit durch die Veränderung der Integrität nicht die Verfügbarkeit und Vertraulichkeit beeinträchtigt werden. Im *Besonderen Teil* wird lediglich auf Informationsmöglichkeiten hingewiesen, welche hiesigen Erachtens bereits durch das IT-Sicherheitsgesetz und das Umsetzungsgesetz der NIS-Richtlinie geschaffen worden sind.

§ 109b Absatz 2 TKG

Es ist unklar, wie eine operative Umsetzung erfolgen soll, ohne dass diese entweder dysfunktional wäre (zu spätes Erkennen) oder zu "Overblocking" führe. X

§ 13 Absatz 7a TMG

In dieser Norm verbleibt die Haftungsfrage bei Nutzung der neu geschaffenen Anordnungsbefugnis, vor allem bei Infrastrukturen im besonderen öffentlichen Interesse und Kritischen Infrastrukturen, ungeklärt.

StGB und StPO Änderungen (allgemein)

Nach gesicherten rechtswissenschaftlichen Erkenntnissen ist eine Verschärfung des Strafrechts kein geeignetes bzw. effektives Mittel zur Reduktion von Straftaten[15] und trägt daher im vorliegenden Fall auch nicht zu mehr IT-Sicherheit bei.

§ 126a StGB

Diese Norm ist sehr weit gefasst und von zweifelhaftem praktischen Nutzen.[16] Die dort genannten "internetbasierten Leistungen" erfassen laut Gesetzesbegründung "alle Dienste, die auf der Netzwerkschicht des OSI-Referenzmodells über das Internet-Protokoll (IP) vermittelt werden". Es beinhaltet dediziert auch das Zugänglichmachen zu solchen Plattformen, auf denen Äußerungsdelikte begangen werden. Damit bezieht sich die Norm also auch auf reguläre Foren, soziale Medien, Videochat-Räume, Virtuelle Private Netzwerke, Chatgruppen in verschlüsselten Messengerdiensten und viele mehr. Da diese Norm sowohl alle technischen internetbasierten Leistungen als auch sämtliche rechtswidrigen Taten (gem. § 11 Absatz 1 Nummer 5 StGB) beinhaltet, wird die Unterscheidung ausschließlich durch die Ausrichtung des Zwecks vorgenommen. Gleichzeitig "begründet § 126a StGB-E damit eine im IT-Strafrecht bisher beispiellose Vorfeldstrafbarkeit".[17]

§ 202e StGB

Es handelt sich hierbei um eine problematische Vorverlagerung der Strafbarkeit zur Versuchsstrafbarkeit. Änderungen zum *Digitalen Hausfriedensbruch* tragen. Dass dies zur Schließung von Schutzlücken oder einer verbesserten Strafverfolgungspraxis führt, darf bezweifelt werden.[18]

Zusätzlich wird weitere Rechtsunsicherheit für IT-Sicherheitsforscher:innen und -Schwachstellenforscher:innen sowie Bug-Bounty Programme geschaffen. Ein Abbau dieser Unsicherheit wäre aber notwendig, um diese Arbeit zu fördern. Damit ist diese Norm möglicherweise sogar kontraproduktiv für die IT-Sicherheit in Deutschland.

§ 202f StGB

X

Die Schwere der Tat an der Anzahl der betroffenen Systeme festzumachen, ist nicht notwendigerweise zielführend. Die Kritikalität der Systeme (z.B. KRITIS, nicht-KRITIS, Infrastrukturen im besonderen öffentlichen Interesse) sollte hier das vorrangige Bewertungskriterium für eine schwere Straftat sein. Ansonsten konstituiert sowohl das Abschalten eines Atomkraftwerks als auch die Erstellung eines Botnetzes bestehend aus 50 vernetzten Zahnbürsten eine schwere Straftat gem. §202e. Auch ist nicht klar ersichtlich, welche dieser durch den Gesetzesentwurf als Straftaten definierten Handlungen auch jetzt schon strafbar sind (u. a. Beeinträchtigung der Funktionsfähigkeit einer kritischen Infrastruktur) und warum die Ausnutzung informationstechnischer Systeme zu diesem Zweck einen Unterschied darstellen soll.

§ 163g StPO

Expert:innen zweifeln stark an der Verfassungskonformität dieser Norm[19]. Weiterhin ist es nicht ersichtlich, inwiefern sie technisch sinnvoll und umsetzbar ist.[20] In Ermangelung der Überwachungsgesamtschau gibt es keine empirische Evidenz die auf eine Notwendigkeit dieser Befugnis hindeutet.

---

[1] Andre Meister und Anna Biselli: IT-Sicherheitsgesetz 2.0: Wir veröffentlichen den Entwurf, der das BSI zur Hackerbehörde machen soll (https://netzpolitik.org/2019/it-sicherheitsgesetz-2-0-wir-veroeffentlichen-den-entwurf-der-das-bsi-zur-hackerbehoerde-machen-soll/)

[2] Bundesanzeiger: Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) (http://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl115s1324.pdf)

[3] Sven Herpig: Sachverständigenstellungnahme im Ausschuss für Inneres und Heimat (https://www.bundestag.de/resource/blob/633906/fb324d240672537e93d53c50171a2388/A-Drs-19-4-255-A-data.pdf) und Sven Herpig: Warum sollte die Polizei Instagram-Passwörter bekommen? (https://www.spiegel.de/netzwelt/netzpolitik/it-sicherheitsgesetz-bundesinnenministerium-will-neue-polizei-befugnisse-a-1262339.html)

[4] Bundesregierung: Koalitionsvertrag zwischen CDU, CSU und SPD (https://www.bundesregierung.de/breg-de/themen/koalitionsvertrag-zwischen-cdu-csu-und-spd-195906)

[5] digitalcourage: Überwachungsgesamtrechnung (https://digitalcourage.de/ueberwachungsgesamtrechnung/sammlung)

[6] Sabine Leutheusser-Schnarrenberger: IT-Sicherheitsgesetz 2.0 – Seehofer bläst zur Attacke (https://www.heise.de/amp/meldung/Gastbeitrag-IT-Sicherheitsgesetz-2-0-Seehofer-blaest-zur-Attacke-4397919.html)

X

[7] Bundesregierung: Koalitionsvertrag zwischen CDU, CSU und SPD (https://www.bundesregierung.de/breg-de/themen/koalitionsvertrag-zwischen-cdu-csu-und-spd-195906)

[8] Sven Herpig: Sachverständigenstellungnahme im Ausschuss für Inneres und Heimat (https://www.bundestag.de/resource/blob/633906/fb324d240672537e93d53c50171a2388/A-Drs-19-4-255-A-data.pdf)

[9] Bundesamt für Sicherheit in der Informationstechnik: Aktiv für mehr Cyber-Sicherheit (https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Ueber_uns/Aktiv_fuer_mehr_Cyber-Sicherheit/aktiv_fuer_mehr_cyber-sicherheit.html)

[10] Amtsblatt der Europäischen Union: RICHTLINIE (EU) 2016/1148 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 6. Juli 2016 (https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016L1148&from=DE)

[11] Bundesgesetzblatt: Gesetzzur Umsetzung der Richtlinie (EU) 2016/1148des Europäischen Parlaments und des Rates vom 6. Juli 2016 (http://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl117s1885.pdf)

[12] Sven Herpig und Julia Schuetze: Mehr IT-Sicherheit für deutsche Wahlen (https://background.tagesspiegel.de/mehr-it-sicherheit-fuer-deutsche-wahlen)

[13] Bundesregierung: Staatsministerium für Kultur und Medien (https://www.bundesregierung.de/breg-de/bundesregierung/staatsministerin-fuer-kultur-und-medien/staatsministerin-und-ihr-amt/aufgaben)

[14] ThingsCon: Trustable Technology Mark (https://www.thingscon.org/trustable-technology-mark/)

[15] z.B. Wolfgang Heinz: Mehr und härtere Strafen? (http://www.uni-konstanz.de/rtf/kis/Heinz_Mehr_und_haertere_Strafen_he306.pdf)

[16] Matthias Bäcker und Sebastian J. Golla: Strafrecht in der Finsternis: Zu dem Vorhaben eines „Darknet-Tatbestands“ (https://verfassungsblog.de/strafrecht-in-der-finsternis-zu-dem-vorhaben-eines-darknet-tatbestands/)

[17] Matthias Bäcker und Sebastian J. Golla: Strafrecht in der Finsternis: Zu dem Vorhaben eines „Darknet-Tatbestands“ (https://verfassungsblog.de/strafrecht-in-der-finsternis-zu-dem-vorhaben-eines-darknet-tatbestands/)

[18] Ulf Buermeyer und Sebastian J. Golla: “Digitaler Hausfriedensbruch” – Der Entwurf eines Gesetzes zur Strafbarkeit der unbefugten Benutzung informationstechnischer Systeme (https://www.ruw.de/suche/kur/Digita-Hausfrieden--Der-Entwur-eines-Gesetz-zur-St-75b3091bb9fc09518a930aa904c2b2fc?crefresh=1)

[19] Jannis Brühl: Passwort oder Beugehaft (https://www.sueddeutsche.de/digital/passwort-it-sicherheit-gesetz-seehofer-beugehaft-gefaengnis-1.4401627)

[20] Sven Herpig: Warum sollte die Polizei Instagram-Passwörter bekommen? (https://www.spiegel.de/netzwelt/netzpolitik/it-sicherheitsgesetz-bundesinnenministerium-will-neue-polizei-befugnisse-a-1262339.html)

X

08. Mai 2019

Autoren:
Sven Herpig

Ansprechpartner:
Dr. Sven Herpig (/de/person/dr-sven-herpig)

Themen:
Internationale Cyber-Sicherheitspolitik (/de/projekt/internationale-cyber-sicherheitspolitik)

Unsere Themen

› (/de/projekt/algorithmen-fuers-gemeinwohl)
› (/de/projekt/arbeitsmarkt-40)
› (/de/projekt/datenoekonomie)
› (/de/projekt/desinformation-der-digitalen-oeffentlichkeit)
› (/de/projekt/digitale-energiewende)

› (/de/projekt/digitale-grundrechte-ueberwachung-transparenz)
› (/de/projekt/digitale-infrastrukturen)
› (/de/projekt/internationale-cyber-sicherheitspolitik)
› (/de/projekt/it-sicherheit-im-internet-der-dinge)
› (/de/projekt/kuenstliche-intelligenz-und-aussenpolitik)

Informationen

› (/de/ueber-uns)
› (/de/newsletter)
› (/de/newsletter)
› (/de/presseanfragen)
› (/de/kontakt)

Follow us

(https://www.facebook.com/snvberlin/)
(https://twitter.com/snv_berlin)
(/de/themen/rss.xml)
(/de/publikationen/rss.xml)
(/de/veranstaltungen/rss.xml)

X

(/node/1409)
(/node/176)
(http://www.make-studio.net/de/)