Vorläufige Bewertung des Referentenentwurfs zum IT-Sicherheitsgesetz 2.0 vom 07.05.2020 und Empfehlungen

Autor:innen[1]

Dr. Sven Herpig, Leiter Internationale Cybersicherheitspolitik bei der Stiftung Neue Verantwortung

und

Jan-Peter Kleinhans, Leiter Technologie & Geopolitik bei der Stiftung Neue Verantwortung

Bereich 5G-Sicherheit/ Vertrauenswürdigkeitserklärung für Hersteller kritischer Komponenten

Die folgende Bewertung befasst sich mit dem Referentenentwurf des Bundesministeriums des Innern, für Bau und Heimat zum Zweiten Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme in der Fassung vom 7. Mai 2020, veröffentlicht auf Netzpolitik.org[2]*.*

[1] Ein Dank geht an die deutsche Cybersicherheitspolitik-Community für die Unterstützung bei der Erstellung dieser Bewertung.
[2] Andre Meister: Seehofer will BSI zur Hackerbehörde ausbauen

Stiftung Neue Verantwortung

A. Gesamtkritik

Im Vergleich zum Referentenentwurf vom 27. März 2019[3] ist bei der vorliegenden Fassung vom 7. Mai 2020 zu begrüßen, dass die Änderungen zum StGB und StPO – und hier im Besonderen § 126a StGB, § 202e StGB, § 202f StGB und § 163g StPO - wie in der vorläufigen Bewertung vom 8. Mai 2019 angeregt[4], ersatzlos gestrichen worden sind. Nach gesicherten rechtswissenschaftlichen Erkenntnissen ist eine Verschärfung des Strafrechts kein geeignetes bzw. effektives Mittel zur Reduktion von Straftaten[5] und hätte in diesem Kontext daher auch nicht zu mehr IT-Sicherheit beigetragen.

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

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

1. IT-Sicherheit für die Gesellschaft durch Verbraucherschutz
2. Evaluierung der bisherigen IT- und Cybersicherheitsmaßnahmen
3. Mobile Incident Response Teams-Strategie
4. Unternehmen im besonderen öffentlichen Interesse
5. Schwachstellenmanagement und -meldewesen
6. Untersuchung der Sicherheit in der Informationstechnik
7. IT-Sicherheit in Digitalisierungsvorhaben
8. Kritische Komponenten und vertrauenswürdige Hersteller
9. Eingriff der Diensteanbieter in die Integrität von Kundensystemen
10. Anordnungsbefugnis gegenüber Kritischen Infrastrukturen und Infrastrukturen im besonderen öffentlichen Interesse
11. Pflichten der Diensteerbringer
12. Staatliche Cybersicherheitsarchitektur

Allgemein ist zu kritisieren, dass die Aktualisierung des Gesetzes ohne eine Evaluierung des vorangegangenen ersten IT-Sicherheitsgesetzes geplant wird, vor allem da ohne jegliche Evidenz von „Erfahrungen aus dem ersten IT-Sicherheitsgesetz“ (s. A. Allgemeiner Teil, II. Wesentlicher Inhalt des Entwurfs) gesprochen wird. Bereits bei dem Entwurf der Cybersicherheitsstrategie für Deutschland 2016 gab es keine Evaluierung der Cybersicherheitsstrategie 2011. Dieses Versäumnis wiegt in dem vorliegenden Vorhaben zum IT-Sicherheitsgesetz 2.0 noch weitaus schwerer, da im Vorgängergesetz sogar

[3] Andre Meister und Anna Biselli: T-Sicherheitsgesetz 2.0: Wir veröffentlichen den Entwurf, der das BSI zur Hackerbehörde machen soll
[4] Sven Herpig: Vorläufige Bewertung des Referentenentwurfs zum IT-Sicherheitsgesetz 2.0
[5] Siehe u. a. Wolfgang Heinz: Mehr und härtere Strafen = mehr Innere Sicherheit! Stimmt diese Gleichung? Strafrechtspolitik und Sanktionierungspraxis in Deutschland im Lichte kriminologischer Forschung

eine Teilevaluierung rechtlich verankert wurde.[6] Die Evaluierung von Maßnahmen ist ein elementarer Bestandteil staatlichen Handelns und sollte auch bei diesem Gesetzgebungsvorhaben durchgeführt werden, bevor eine Kompetenz- und Anforderungsausweitung verabschiedet wird. Der vorliegende Entwurf sieht zusätzlich weder eine Befristung noch eine gesonderte Evaluierung vor (Begründung, A. Allgemeiner Teil, VII. Befristung; Evaluierung). Stattdessen wird nur auf eine zukünftige gemeinsame Evaluierung beider IT-Sicherheitsgesetze ohne Spezifika verwiesen. Offensichtlich wird im Bereich der IT- und Cybersicherheitspolitik weiterhin versucht, sicherheitsbehördliche Kompetenzen auszubauen, ohne die Effektivität existierender Kompetenzen vorher zu evaluieren.
Der aktuelle Gesetzesentwurf ignoriert weiterhin die im Koalitionsvertrag[7] festgelegte "gleichzeitige und entsprechende Ausweitung der parlamentarischen Kontrolle" bei Ausweitung der Befugnisse der Sicherheitsbehörden. Das ist höchst problematisch, da die Bundesregierung bislang noch immer nicht die vom Bundesverfassungsgericht 2010 angeregte Gesamtschau der staatlichen Überwachungsmaßnahmen ("Überwachungsgesamtrechnung")[8] vorgelegt hat. Eine Befugnis-Erweiterung der Sicherheitsbehörden im IT-Sicherheitsgesetz 2.0 sollte unbedingt durch geeignete und angemessene Schutzmechanismen und Kontrollmaßnahmen begrenzt werden.

Auch auf die im Koalitionsvertrag vereinbarte Stärkung des Bundesamts für Sicherheit in der Informationstechnik "in seiner Rolle als unabhängige und neutrale Beratungsstelle für Fragen der IT-Sicherheit"[9] wird in dem Entwurf nicht eingegangen. Der Entwurf sollte zumindest eine Prüfung unterschiedlicher Unabhängigkeitsmodelle (z. B. Statistisches Bundesamt oder Bundesbeauftragter für den Datenschutz und die Informationsfreiheit)[10] vorsehen.

Zu dem Mangel empirischer Evidenz bei der Normengestaltung[11] und fehlender Berücksichtigung der Vorgaben aus dem Koalitionsvertrag kommen weitere Defizite, auf die im Folgenden eingegangen wird. Eine Überarbeitung des Referentenentwurfs wäre daher notwendig und zielführend, um die Cyber- und Informationssicherheit in Deutschland nachhaltig zu stärken.

[6] Bundesanzeiger: Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz)
[7] Bundesregierung: Koalitionsvertrag zwischen CDU, CSU und SPD
[8] digitalcourage: Überwachungsgesamtrechnung
[9] Bundesregierung: Koalitionsvertrag zwischen CDU, CSU und SPD
[10] Sven Herpig: Sachverständigenstellungnahme im Ausschuss des Deutschen Bundestags für Inneres und Heimat
[11] Sven Herpig: Sachverständigenstellungnahme im Ausschuss des Deutschen Bundestags für Inneres und Heimat

Stiftung
Neue
Verantwortung

B. Einzelkritik (nicht abschließend)

1. IT-Sicherheit für die Gesellschaft durch Verbraucherschutz

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

Der Entwurf definiert den Schutz von Gesellschaft als eines der Kernziele des Gesetzes. Als Hauptmaßnahme zum Schutz der Bürger:innen, und der damit verbundenen größten Personalaufwendung, führt der Entwurf die Einführung des „IT-Sicherheitskennzeichens“ an. Allerdings wird das IT-Sicherheitskennzeichen nicht direkt zu einer Erhöhung der IT- und Cybersicherheit in Deutschland führen. Eine indirekte Erhöhung der IT- und Cybersicherheit wäre bei verpflichtenden IT-Sicherheitssiegeln zumindest durch die Beeinflussung der Kaufentscheidung und des damit einhergehenden Einflusses auf Hersteller, die sich um eine verbesserte IT-Sicherheit ihrer Produkte bemühen müssten, gegeben.[12] Wenn eine Kennzeichnung mit dem IT-Sicherheitskennzeichen in Verbindung mit dem elektronischen Beipackzettel freiwillig ist, signalisiert es nur, wie (un)sicher ein Produkt ist. Weder die Produkte noch die Bürger:innen/Gesellschaft werden damit direkt sicherer. Zugespitzt bedeutet dies, dass IT-Produkte, deren Schutzmechanismen im Entwurf selbst als „faktisch wirkungslos“ bezeichnet werden, weiterhin verkauft werden dürften und nur auf Basis von Freiwilligkeit des Herstellers ein entsprechendes IT-(Un)Sicherheitskennzeichen auf der Verpackung tragen würden. Gleichzeitig entsteht durch die in §§ 9a und 3 Absatz 14 BSIG-E erwähnten Aufgaben ein hoher Mehraufwand für das Bundesamt für Sicherheit in der Informationstechnik. Es ist zu bezweifeln, dass der Ertrag den Aufwand beim freiwilligen IT-Sicherheitskennzeichen rechtfertigt. Die Maßnahme ist möglicherweise effektiv, aber keineswegs effizient. Vor dem Hintergrund der nach wie vor herrschenden Knappheit an IT-Sicherheitsfachkräften im öffentlichen Dienst sollte diese Maßnahme dringend überdacht werden.

Empfehlung: Die Bundesregierung sollte darauf hinarbeiten, dass bekanntermaßen unsichere und nicht mehr absicherbare IT-Produkte überhaupt nicht in den Handel gelangen dürfen.[13] Weiterhin sollten konkrete Maßnahmen ergriffen werden, die direkt für eine höhere Sicherheit der Bürger:innen sorgen, wie z. B. eine voreingestellte Netzwerksegmentierung bei Routern (Heimnetz/ IoT-Geräte). Die Idee des IT-Sicherheitskennzeichens sollte stattdessen direkt auf EU-Ebene angegangen werden, damit der Einsatz von verpflichtenden statt nur freiwilligen Siegeln ermöglicht werden kann (siehe „Warenverkehrsfreiheit“). Gleichzeitig muss sichergestellt werden, dass ein (freiwilliges) IT-Sicherheitskennzeichen nicht mit höherwertigen Zertifizierungen von Produkten vermischt wird.

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

2. Evaluierung der bisherigen IT- und Cybersicherheitsmaßnahmen

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

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

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

3. Mobile Incident Response Teams-Strategie

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

Die Mobile Incident Response Teams (MIRTs) des Bundesamtes für Sicherheit in der Informationstechnik sind ein Kernelement reaktiver Maßnahmen in der deutschen Cyber- und IT-Sicherheitspolitik. Der Mehrwert der MIRTs für die deutsche Cyber- und IT-Sicherheitspolitik ist für die Öffentlichkeit nachvollziehbar, wie u. a. der Fall des Lukaskrankenhauses in Neuss[14] gezeigt hat.

Empfehlung: Ein Ausbau der MIRTs ist zu unterstützen, da für diese eine breite Fachexpertise – zum Beispiel für die unterschiedlichen Systeme Kritischer Infrastrukturen – bereitgehalten werden muss. Der genannte Ausbau der Teams wäre eine effiziente Investition der im Entwurf insgesamt vorgesehenen Personalressourcen. Es ist dabei jedoch unklar, wie viele MIRTs notwendig sind, u. a. wegen Bereitschaftszeiten und Spezialexpertise. Es sollte daher dargelegt werden, welcher Plan hinter dem Ausbau der MIRTs steht und wie viele dieser Teams zu welchem Zeitpunkt für welche Einsatzgebiete (Regierung, KRITIS o. ä.) bereitstehen müssen. Dieser Plan sollte auch Transparenz über Einsatzstatus, Aufgabenteilung und Einsatzgebiete der „Quick Reaction Forces“ des Bundeskriminalamts, der „Mobile Cyber-Teams“ des Bundesamts für Verfassungsschutz und analoger Teams des Militärischen Abschirmdiensts und Bundesnachrichtendiensts herstellen.[15] Zudem sollte eine Einbettung des Konzepts des Cyber-Hilfswerks[16] in diesen Plan geprüft werden. Eine Integration des Mobile Incident Response Team Plans in den „Gesamtplan für die Reaktionsmaßnahmen des Bundes“ gem. § 5c BSIG-E wäre zielführend.

[14] Noah Gottschalk: Wenn eine Klinik ohne Computer arbeiten muss
[15] Bundesministerium des Innern: Cyber-Sicherheitsstrategie für Deutschland 2015
[16] AG KRITIS: Cyber-Hilfswerk (CHW)

Stiftung Neue Verantwortung

4. Unternehmen im besonderen öffentlichen Interesse

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

Es ist unklar, in welchem Verhältnis die im Gesetz genannten „Institutionen im besonderen staatlichen Interesse" (INSI)[17] zu den im Entwurf erstmals erwähnten „Unternehmen im besonderen öffentlichen Interesse" gem. § 8f BSIG-E und der „Infrastruktur im besonderen öffentlichen Interesse“ gem. § 109a Abs 8 TKG-E stehen. Weder in der EU NIS-Richtlinie[18] noch in dem entsprechenden Umsetzungsgesetz[19] finden sich diese Begrifflichkeiten wieder. Im Umsetzungsgesetz wird lediglich einmal von „informationstechnischen Systemen von besonderem öffentlichem Interesse" gesprochen (§ 5a Absatz 2 BSIG). Diese Inkonsistenzen wirken einer Harmonisierung entgegen und verstärken die Komplexität durch die unilaterale Einführung einer weiteren „Schutzklasse“. Weiterhin ist nicht ersichtlich, warum politische Parteien von der KRITIS-Regulierung und der Regulierung für die „Unternehmen im besonderen öffentlichen Interesse“ ausgenommen sein sollten. Parteien sind Kernelemente des politischen Systems, und damit kritisch für die Demokratie in Deutschland. Sie sollten als solche daher entsprechend hohe IT-Sicherheitsstandards erfüllen.[20]

Empfehlung: Die Bundesregierung muss Transparenz bzgl. der „Institutionen im besonderen staatlichen Interesse“ im Vergleich zu „Unternehmen im besonderen öffentlichen Interesse“ und „Infrastruktur im besonderen öffentlichen Interesse“ schaffen. Gleichzeitig sollten die Kategorien der deutschen Gesetzgebung nicht von der EU-Harmonisierung abweichen, weshalb eine zusätzliche, unilaterale Einführung der „Unternehmen im besonderen öffentlichen Interesse“ o. ä. verworfen werden sollte. Auch inhaltlich erscheint diese zusätzliche Kategorie nicht sinnvoll: Entweder werden Unternehmen als kritisch genug betrachtet, um sie bzgl. IT-Sicherheit zu regulieren und folglich unter der KRITIS-Regulierung zu subsumieren, oder aber sie werden als nicht relevant genug eingeordnet, um bzgl. IT-Sicherheit reguliert zu werden. In diesem Fall können sie dann unter den bestehenden, unbestimmten Rechtsbegriff der „Institutionen im besonderen staatlichen Interesse“ fallen. Eine Ausdifferenzierung kann bei Aufnahme in die KRITIS-Regulierung über die branchenspezifischen Sicherheitsstandards[21] stattfinden. Darüber hinaus ist zu prüfen, ob politische Parteien wegen ihrer Relevanz für das Funktionieren des deutschen Staates in die KRITIS-Regulierung aufgenommen werden sollten. Sollte die Bundesregierung an der Einführung der zusätzlichen Kategorie „Unternehmen im besonderen öffentlichen Interesse“ festhalten, so ist zumindest § 10 Absatz 5 BSIG-E um die Beteiligung der organisierten Zivilgesellschaft zu erweitern.

[17] Bundesamt für Sicherheit in der Informationstechnik: Allianz für Cyber-Sicherheit Registrierung
[18] Amtsblatt der Europäischen Union: RICHTLINIE (EU) 2016/1148 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 6. Juli 2016
[19] Bundesgesetzblatt: Gesetz zur Umsetzung der Richtlinie (EU) 2016/1148des Europäischen Parlaments und des Rates vom 6. Juli 2016
[20] Sven Herpig und Julia Schuetze: Mehr IT-Sicherheit für deutsche Wahlen
[21] Bundesamt für Sicherheit in der Informationstechnik: Branchenspezifische Sicherheitsstandards

5. Schwachstellenmanagement und -meldewesen

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

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

Empfehlung: Empfohlen wird ein Verweis auf eine separate Verordnung o. ä., die den Umgang mit Schwachstellen durch Behörden dezidiert regelt, anstatt einer Regelung der Prozesse über die im Entwurf angeführten Normen. Zudem wird eine Einführung des seit Jahren in Planung befindlichen Schwachstellenmanagements des Bundesministeriums des Innern, für Bau und Heimat am Beispiel des von der Stiftung Neue Verantwortung vorgelegten Entwurfs empfohlen[22]. Gleichzeitig sollte ein Errichtungsgesetz für die Schwachstellen-verarbeitende Zentrale Stelle für Sicherheit in der Informationstechnik erarbeitet werden. Das ist dringend notwendig, da die Behörde ihre invasive Tätigkeit momentan ohne eine solche Gesetzesgrundlage ausübt. In den Gesetzen aller Schwachstellen-verarbeitenden Sicherheitsbehörden auf Bundesebene (u. a. Bundesnachrichtendienst, Bundeskriminalamt, Bundespolizei, Bundesamt für Verfassungsschutz, Bundeswehr, Zentrale Stelle für Sicherheit in der Informationstechnik) muss eine Reziprozität bzgl. der Weitergabe von Schwachstellen ergänzt werden: Während das Bundesamt für Sicherheit in der Informationstechnik gem. § 3 Absatz 1 Satz 13 BSIG andere Bundesbehörden bei der Wahrnehmung ihrer gesetzlichen Aufgaben unterstützen muss, sind diese Bundesbehörden ihrerseits nicht verpflichtet, das Bundesamt für Sicherheit in der Informationstechnik durch die Weitergabe der von ihnen gefundenen oder erworbenen Schwachstellen zu unterstützen. Dies ist allerdings eine Grundvoraussetzung für die Wahrnehmung der gesetzlichen Aufgaben des Bundesamtes für Sicherheit in der Informationstechnik.

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

[22] Sven Herpig: Schwachstellen-Management für mehr Sicherheit

6. Untersuchung der Sicherheit in der Informationstechnik

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

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

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

7. IT-Sicherheit in Digitalisierungsvorhaben

§ 8 Absatz 4 BSIG-E

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

Empfehlung: Die Angabe „frühzeitig“ sollte präzisiert bzw. ein grober Zeitraum inkludiert werden. Weiterhin sollte ermöglicht werden, dass andere Behörden die Unterstützung des Bundesamts für Sicherheit in der Informationstechnik direkt und ohne vorherigen Kontakt zum Bundesministerium des Innern, für Bau und Heimat ersuchen können. Das würde auch die im Koalitionsvertrag angekündigte Stärkung des Bundesamts für Sicherheit in der Informationstechnik "in seiner Rolle als unabhängige und neutrale Beratungsstelle für Fragen der IT-Sicherheit"[23] fördern.

[23] Bundesregierung: Koalitionsvertrag zwischen CDU, CSU und SPD

8. Kritische Komponenten und vertrauenswürdige Hersteller

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

Die sehr breite Definition von „kritischen Komponenten“ in Verbindung mit der Garantieerklärung über die „gesamte Lieferkette des Herstellers“ auf Basis einer nicht näher definierten späteren Allgemeinverfügung des Bundesministeriums des Innern, für Bau und Heimat macht eine Bewertung dieser Norm ohne weitere Details schwer möglich. Der Anwendungsbereich dieser Norm geht weit über die technische IT- und Cybersicherheit hinaus, für die das Bundesamt für Sicherheit in der Informationstechnik – und damit das BSIG – verantwortlich ist. Dies wird unter anderem dadurch deutlich, dass in diesem Kontext das Bundesministerium des Innern, für Bau und Heimat und nicht mehr das Bundesamt für Sicherheit in der Informationstechnik genannt wird. Diese Perspektive wird u. a. dadurch verstärkt, dass der Text nicht mehr auf die „Grundwerte der Informationssicherheit“ (Verfügbarkeit, Vertraulichkeit und Integrität)[24] verweist, sondern „Vertraulichkeit“ weglässt und stattdessen die Kategorien „Funktionsfähigkeit“ und „Sicherheit“ anführt. Es handelt sich hierbei um außen- und sicherheitspolitische Normen, die nicht über das BSIG geklärt werden sollten.

In der Begründung zu § 9b BSIG-E wird zu Recht festgestellt, dass die Zertifizierung der IT-Sicherheit einer kritischen Komponente nicht die Überprüfung der Vertrauenswürdigkeit eines Herstellers umfasst und beides zwingend getrennt betrachtet werden muss. Die aufgelisteten Kriterien (§ 9b Absatz 4 BSIG-E) zur Einschätzung der Vertrauenswürdigkeit eines Herstellers adressieren jedoch ausschließlich technische Risiken (Penetrationstests, Schwachstellen-Management, “Hintertüren”). Eine ganzheitliche Einschätzung der Vertrauenswürdigkeit eines Herstellers wird dadurch verfehlt.

Weiterhin besagt § 9b Absatz 4 Punkt 5 BSIG-E, dass ein Hersteller nicht vertrauenswürdig sei, wenn „die kritische Komponente über technische Eigenschaften verfügt, die geeignet sind, missbräuchlich auf die Sicherheit, Integrität, Verfügbarkeit oder Funktionsfähigkeit der Kritischen Infrastruktur einwirken zu können.” Dieses Kriterium ist nicht geeignet, um die Vertrauenswürdigkeit eines Herstellers einzuschätzen, da Netzwerkkomponenten immer eine solche Fernwartungsschnittstelle besitzen, über die die Netzwerkkomponente kontrolliert werden kann. Eine solche Schnittstelle kann in jedem Fall durch Betreiber und unter Umständen auch durch den Komponentenhersteller benutzt werden, um „missbräuchlich auf die Sicherheit, Integrität, Verfügbarkeit oder Funktionsfähigkeit der Kritischen Infrastruktur” einzuwirken. Das Verbot eines solchen Fernwartungszugangs ist nicht möglich. Damit bleibt das Kriterium wirkungslos.[25] Die Vertrauenswürdigkeit eines Herstellers muss, unabhängig von der IT-Sicherheitszertifizierung der Komponenten, anhand von nicht-technischen Kriterien überprüft werden. Eine solche Überprüfung kann nicht durch das Bundesamt für Sicherheit in der Informationstechnik geleistet werden, sondern muss zwingend durch mehrere Ressorts erfolgen. Die Grundlage hierfür sollte daher nicht im BSIG-E gelegt werden.

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

[24] Bundesamt für Sicherheit in der Informationstechnik: IT-Grundschutz Glossar
[25] Jan-Peter Kleinhans: Whom to trust in a 5G world?

9. Eingriff der Diensteanbieter in die Integrität von Kundensystemen

§ 109a Absatz 8 TKG-E in Verbindung mit § 109a Absätze 4,5 und 6 sowie § 149 Absatz 1 TKG

Es handelt sich hierbei um einen angeordneten Eingriff in das Computergrundrecht[26]. Es ist unklar, wie die operative Umsetzung aussähe und welche Schutzmechanismen ergriffen würden, um die Verfügbarkeit und Vertraulichkeit der betroffenen Datenverarbeitungssysteme durch die Veränderung der Integrität nicht zu beeinträchtigen. Darüber hinaus leistet Absatz 8 im Sinne der IT- und Cybersicherheit keinen erkennbaren zusätzlichen Schutz zu den Maßnahmen gem. der Absätze 4, 5 und 6. Eine Nichteinhaltung ist mit Bußgeldforderungen belegt.

Empfehlung: § 109a Absatz 8 TKG-E sollte ersatzlos gestrichen werden.

10. Anordnungsbefugnis gegenüber Diensteanbietern

§ 13 Absatz 7a TMG-E

In dieser sehr weit und unpräzise gefassten Norm (Beispiel: „Vielzahl von Nutzern“) bleibt die Haftungsfrage bei Nutzung der neu geschaffenen Anordnungsbefugnis ungeklärt. Dies ist vor dem Hintergrund eines möglicherweise sehr hohen Erfüllungsaufwands - vgl. Reichweite der Norm in Verbindung mit der Eingriffstiefe - für Dritte sehr problematisch.

Empfehlung: Eine Klärung der Haftungsfrage – vor allem vor dem Hintergrund der Eingriffstiefe der Anordnungen – sowie die klare Abgrenzung der unterschiedlichen Kategorien voneinander scheinen zwingend notwendig. Weiterhin muss geklärt werden, wie weit die Anordnungsbefugnis reicht (u. a. bis zur Produktentwicklung). Entsprechend des Umfangs der Norm muss dem Erfüllungsaufwand Dritter mit adäquaten Haftungsregelungen oder Ausgleichsmaßnahmen entgegengewirkt werden.

11. Pflichten der Diensteerbringer

§ 15b Abs 1 TMG-E

Es handelt sich hierbei um eine zu weitgefasste Norm, die unter anderem auf einer unklaren Begründung des Staatswohls – vgl. § 15b Abs 1 Satz 3 TMG-E – basiert. Problematisch ist weiterhin, dass keine Bereichsausnahmen für Tätigkeiten im öffentlichen Interesse, zum Beispiel für die Arbeit der Presse, vorgesehen sind. Es ist anzuzweifeln, dass Diensteerbringer in der Vergangenheit einer entsprechenden Verpflichtung gem. § 15b Abs 1 TMG-E wissentlich nicht gefolgt sind. Weiterhin stellt § 15b Abs 2 TMG-E ohne Anordnung durch zuständige Behörden, zum Beispiel durch das Bundeskriminalamt, einen möglicherweise unverhältnismäßigen Aufwand für die Diensteerbringer dar.

Empfehlung: Es ist zu prüfen, ob eine empirische Grundlage für § 15b Abs 1 TMG-E gewährleistet ist, gemäß derer Diensteerbringer dieser Pflicht nicht nachgekommen sind. § 15b Abs 2 TMG-E sollte

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

ausschließlich eine zwingende und nicht optionale Anordnung der zuständigen Stellen vorsehen. Die Norm sollte um § 15b Abs 4 TMG-E ergänzt werden, der eine Ausnahme von den Absätzen 1-3 vorsieht, sobald die zur Veröffentlichung vorgesehenen Daten dem öffentlichen Interesse dienen. Dies sollte insbesondere dann gelten, wenn das Handeln im Einklang mit § 5 GeschGehG und dem geltenden Datenschutzrecht, sowie den hierin enthaltenen Bereichsausnahmen medialer Arbeit (beispielhaft: § 12 LPG NRW, § 59 RStV) steht.

12. Staatliche Cybersicherheitsarchitektur

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

Im Referentenentwurf heißt es, dass der Inhalt des Entwurfs der „deutschen IT-Sicherheitsarchitektur" entspricht. Auf welche Grundlage sich dieser Terminus bezieht, bleibt dabei völlig unklar. Die einzig bisher bekannte Übersicht zur staatlichen Cybersicherheitsarchitektur in Deutschland wurde von der Stiftung Neue Verantwortung veröffentlicht.[27] Der Referentenentwurf verliert unabhängig davon kein Wort über eine notwendige Reform der offensichtlich dysfunktionalen, zentralen Akteure der deutschen Cybersicherheitsarchitektur, dem Cyber-Abwehrzentrum und dem Cyber-Sicherheitsrat.

Empfehlung: Das IT-Sicherheitsgesetz 2.0 sollte genutzt werden, um die Strukturen des Cyber-Abwehrzentrums und des Cyber-Sicherheitsrats zu klären und eine rechtliche Grundlage für die Arbeit dieser Institutionen, und der Zentralen Stelle für Informationstechnik im Sicherheitsbereich, zu schaffen. Dies sollte unter anderem Kooperationsmöglichkeiten und -grenzen, Verantwortlichkeiten, Aufgaben und Verortung in der deutschen Cybersicherheitsarchitektur beinhalten. Hierzu gehört beispielsweise die Trennung zwischen operativen und nicht operativen Aufgaben im Bereich der Cybersicherheit (vgl. u. a. BVerfG Leitsätze zum Urteil des Ersten Senats vom 19. Mai 2020)[28]. Weiterhin sollte die Bundesregierung einen Plan zu Weiterentwicklung der deutschen Cybersicherheitsarchitektur vorlegen, insbesondere vor dem Hintergrund der Gründung immer neuer Institutionen wie der Zentralen Stelle für Sicherheit in der Informationstechnik, der Agentur für Sprunginnovationen, der Cyberagentur, dem Zentrum für Digitalisierungs- und Technologieforschung der Bundeswehr und vielen mehr, und damit möglicherweise entstehender unklarer Verantwortlichkeiten und Parallelstrukturen entgegenwirken.

[27] Sven Herpig und Rebecca Beigel: Akteure und Zuständigkeiten in der deutschen Cybersicherheitspolitik
[28] Bundesverfassungsgericht: Leitsätze zum Urteil des Ersten Senats vom 19. Mai 2020 - 1 BvR 2835/17 – [5. Leitsatz]