COT Legal

Claudia Otto
Rechtsanwältin
Bockenheimer Landstraße 2-4
60306 Frankfurt am Main
Telefon: +49 69 667 748 360
Telefax: +49 69 667 748 450
Mail: claudia.otto@cot.legal
Web: https://cot.legal

Stellungnahme

zum

Entwurf eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (Zweites IT-Sicherheitsgesetz – IT-SiG 2.0)

vom 9. Dezember 2020

Der Referentenentwurf des Bundesministeriums des Inneren, für Bau und Heimat vom 1. Dezember 2020 hebt mit den ersten Sätzen „die Gewährleistung der Cyber- und Informationssicherheit" als „ein Schlüsselthema für Staat, Wirtschaft und Gesellschaft" hervor. Gemeint ist das Ziel einer sicheren Infrastruktur, auf der eine dauerhaft funktionierende Informations- und Kommunikationstechnik aufbauen kann. Staat, Wirtschaft und Gesellschaft sind in Quantität und Qualität zunehmenden „Cyber-Angriffen" ausgesetzt. Um diesen wirksam entgegentreten zu können, sieht das IT-SiG 2.0 neue Pflichten von Unternehmen und neue Befugnisse des Bundesamts für Sicherheit in der Informationstechnik (BSI) vor. Unter anderem soll das BSI Sniffing betreiben (durch sog. Portscans) und Fallen (sog. Honeypots) stellen dürfen. Außerdem soll ein einheitliches IT-Sicherheitskennzeichen eingeführt werden. Der Verbraucherschutz soll dementsprechend in den Aufgabenkatalog des BSI übernommen werden.

Dem Schutzgedanken bezüglich Staat, Wirtschaft und Gesellschaft stehen verfassungsrechtlich begründete Schutzinteressen der von Maßnahmen potentiell betroffenen Unternehmen gegenüber. Es bestehen Bedenken im Hinblick auf die Verfassungsmäßigkeit enthaltener Befugnisse.

Das Bundesministerium hat den Referentenentwurf am 2. Dezember 2020 zur Diskussion gestellt. Stellungnahmen können bis 9. Dezember 2020 eingereicht werden. In der Kürze der Zeit ist eine umfassende Stellungnahme zu 92 Seiten nicht möglich. Daher werden nachstehend nur spezifische Probleme herausgehoben und kommentiert. Die Stellungnahme ist nicht dahingehend zu verstehen, dass Unkommentiertes als unproblematisch angesehen wird.

I. Verfassungsrechtliche Bedenken

Der Entwurf des IT-SiG 2.0 erweckt beim Studium Bedenken im Hinblick auf seine Vereinbarkeit mit dem Grundgesetz, insbesondere mit dem Bestimmtheitsgebot, Art. 20 Abs. 3 GG. Rechtsanwender müssen die Folgen eines Gesetzes hinsichtlich Inhalt, Zweck und Ausmaß verstehen, vorhersehen und in ihre Entscheidungen einstellen können. Dies ist bei den nachstehenden, exemplarisch herausgegriffenen Beispielen nicht der Fall.

1. Wer Eingriffsadressat sein kann ist unklar

Ein wesentliches Hauptproblem des Referentenentwurfs ist, dass nicht eindeutig ist, welche Unternehmen von Maßnahmen auf Grundlage des IT-SiG 2.0 betroffen sein können. Dies wird an dem unbestimmten Begriff des „Unternehmen im besonderen öffentlichen Interesse" besonders deutlich. Es fehlt an einem Maßstab, anhand dessen diese Eigenschaft und damit auch die eigene Betroffenheit bestimmt werden kann.

> *(14) [1]Unternehmen im besonderen öffentlichen Interesse sind Unternehmen, die nicht Betreiber Kritischer Infrastrukturen nach Absatz 10 sind und,*
>
> *1. die Güter nach § 60 Absatz 1 Nummer 1 bis 5 der Außenwirtschaftsverordnung in der jeweils geltenden Fassung herstellen oder entwickeln,*
>
> *2. die nach ihrer inländischen Wertschöpfung zu den größten Unternehmen in Deutschland gehören und daher von erheblicher volkswirtschaftlicher Bedeutung für die Bundesrepublik Deutschland sind oder*
>
> *3. die Betreiber eines Betriebsbereichs der oberen Klasse im Sinne der Störfall-Verordnung in der jeweils geltenden Fassung sind, oder nach § 1 Absatz 2 der Störfall-Verordnung diesen gleichgestellt sind.*
>
> *[2]Die Unternehmen im besonderen öffentlichen Interesse nach Nummer 2 werden durch die Rechtsverordnung nach § 10 Absatz 5 bestimmt, in der festgelegt wird, welche wirtschaftlichen Kennzahlen bei der Berechnung der inländischen Wertschöpfung*

> *heranzuziehen sind, mit welcher Methodik die Berechnung zu erfolgen hat und welche Schwellenwerte maßgeblich dafür sind, dass ein Unternehmen zu den größten Unternehmen in Deutschland im Sinne der Nummer 2 gehört."*

Der Begriff der „*erheblichen volkswirtschaftlichen Bedeutung*" in Ziffer 2 ist zu unbestimmt, um auf ihm eine Legaldefinition aufzubauen. „*Nach ihrer inländischen Wertschöpfung*" ist widersprüchlich, weil Wertschöpfung in der Volkswirtschaftslehre als die Summe der in einem bestimmten Zeitraum in den einzelnen Wirtschaftsbereichen der Volkswirtschaft hergestellten Güter und Leistungen[1] verstanden wird. Nicht jedoch als die Güter und Leistungen eines Unternehmens allein. Nachvollziehbarer wäre das Abstellen auf den Anteil eines Unternehmens an dem jeweiligen Wirtschaftsbereich, der, ausweislich der BSI-KritisV, klar bestimmt werden kann. Es bestehen nicht zuletzt praktische Bedenken, ob die Bedeutung eines Unternehmens allein an wirtschaftlichen Kennzahlen festgemacht werden kann, die Schwankungen unterliegen. Unklar ist, welche Auswirkungen Schwankungen im nicht klar definierbaren Grenzbereich haben und ob ein „On/Off" der Anwendbarkeit des Gesetzes zielführend im Hinblick auf die „Gewährleistung der Cyber- und Informationssicherheit" als „Schlüsselthema für Staat, Wirtschaft und Gesellschaft" sein kann. Die vorrangige Orientierung am Tätigkeitsbereich wäre nicht zuletzt in Gesamtschau mit den Ziffern 1 und 3 systematisch stimmig.

Die in Satz 2 vorgesehene Rechtsverordnung vermag die Unbestimmtheit des § 2 Abs. 14 S. 1 Nr. 2 BSIG-E aus vorstehenden Gründen nicht zu beseitigen. § 2 Abs. 14 S. 1 Nr. 2 und S. 2 BSIG-E sollten daher überdacht werden.

2. Welche bußgeldrelevanten Vorkehrungen Unternehmen treffen müssen ist unklar

Beispielhaft soll hier der neue § 8a Abs. 1a BSIG-E angeführt werden. Dieser lautet wie folgt:

> *„(1a) Die Verpflichtung nach Absatz 1 Satz 1, angemessene organisatorische und technische Vorkehrungen zu treffen, umfasst spätestens ein Jahr nach Inkrafttreten dieses Gesetzes auch den Einsatz von Systemen zur Angriffserkennung. Die eingesetzten Systeme zur Angriffserkennung müssen geeignete Parameter bzw. Merkmale aus dem laufenden Betrieb kontinuierlich und automatisch erfassen und auswerten. Sie sollten dazu in der Lage sein, fortwährend Bedrohungen zu identifizieren und zu vermeiden sowie für eingetretene Störungen geeignete Beseitigungsmaßnahmen vorsehen. Absatz 1 Satz 2 und 3 gelten entsprechend.*

Diese Verpflichtung wird durch eine Bußgeldvorschrift, § 14 Abs. 1 Nr. 2 BSIG-E flankiert: Ordnungswidrig handelt hiernach, wer vorsätzlich oder fahrlässig entgegen § 8a Abs. 1a BSIG-E

> *„eine dort genannte Vorkehrung oder Maßnahme nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig trifft."*

In der Begründung auf Seite 67 f. wird hierzu ausgeführt:

> *„§ 8a Absatz 1a ergänzt die Verpflichtung der Betreiber Kritischer Infrastrukturen, angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, nun auch ausdrücklich um Systeme zur Angriffserkennung. Diese Systeme stellen eine effektive Maßnahme zur Begegnung von Cyber-Angriffen dar und unterstützen insbesondere die Schadensreduktion.*
>
> *Bereits heute ist eine große Anzahl von Systemen zur Angriffserkennung verfügbar. Diese unterscheiden sich u.a. in den Verfahren zur Detektion und sind für unterschiedliche Einsatzszenarien optimiert. Unterschiede liegen z.B. in den jeweils untersuchten Daten, die*

[1] https://www.bpb.de/nachschlagen/lexika/lexikon-der-wirtschaft/21123/wertschoepfung.

> *beispielsweise an den Übergängen zu öffentlichen Netzen, vom netzwerkinternen Datenverkehr oder auch von internen Daten der IT-Systeme erhoben werden. Ebenso unterscheidet sich die Methodik zur Erkennung von Cyber-Angriffen. Hierbei gibt es beispielsweise den Abgleich mit statischen Mustern zu Software und Kommunikationen, von denen bekannt ist, dass sie im Zusammenhang mit Cyber-Angriffen stehen. Es werden auch generische Muster sowie Verfahren der künstlichen Intelligenz eingesetzt, um Hinweise auf Cyber-Angriffe zu erhalten. Eine weitere Methode ist es, den störungsfreien Betrieb zu erfassen und dann Abweichungen von diesem Zustand zur Detektion zu verwenden (so genannte Anomaliedetektion)."*[2]

Auch wenn gegen den Einsatz von Systemen zur Angriffserkennung keine Einwände bestehen, so soll doch auf innewohnende Widersprüche hingewiesen werden. Auf Widersprüche können weder Gesetzespflichten noch Ordnungswidrigkeiten gestützt werden:

Problematisch ist zunächst, dass die „Muss-Vorschrift" § 8a Abs. 1a S. 2 BSIG-E auf *„geeignete Parameter bzw. Merkmale aus dem laufenden Betrieb"* Bezug nimmt, die *„kontinuierlich und automatisch"* erfasst und ausgewertet werden. Die Begründung erklärt zu Systemen zur Angriffserkennung lediglich:

> *„Diese Systeme untersuchen automatisiert Daten aus den IT-Systemen, zu dessen Schutz sie eingesetzt werden."*[3]

Es stellt sich die Frage, warum die „Muss-Vorschrift" sich auf etwas bezieht, das lediglich systemeigene Informationen berührt. Mit *false positives*, also falschem Alarm, wäre in der Folge häufiger zu rechnen. Nicht in jeder Unregelmäßigkeit liegt schließlich ein Angriff. Dass der Fokus bei der Angriffserkennung vielmehr auf Informationen „von außen" liegen sollte, wurde grundsätzlich erkannt:

> *„Unternehmen benötigen für den Einsatz von Systemen zur Angriffserkennung Informationen, die sich als Erkennungsmuster zu Cyber-Angriffen einsetzen lassen. Der Einsatz der Systeme zur Angriffserkennung erfordert, dass die eingesetzten Erkennungsmuster ständig aktuell gehalten werden."*[4]

Hier scheint aber lediglich § 8a Abs. 1a S. 3 BSIG-E anzuknüpfen mit

> *„Sie sollten dazu in der Lage sein, fortwährend Bedrohungen zu identifizieren und zu vermeiden sowie für eingetretene Störungen geeignete Beseitigungsmaßnahmen vorsehen."*

Der Wortlaut, der sich nicht direkt an den Verpflichteten richtet, liest sich wie eine Empfehlung. Das Nichtbefolgen einer Empfehlung kann jedoch nicht Ordnungswidrigkeit sein. Die Auswertung eigener Systemdaten und eine Empfehlung zur Detektion bzw. Vermeidung von Bedrohungen stellen keine

> *„effektive Maßnahme zur Begegnung von Cyber-Angriffen dar und unterstützen insbesondere die Schadensreduktion"*[5]

nicht. Ihr Fehlen darf keinen Bußgeldtatbestand – wie hier des § 14 Abs. 1 Nr. 2 BSIG-E erfüllen.

Der Referentenentwurf scheint nicht zuletzt den Einsatz von „Verfahren der künstlichen Intelligenz" als verpflichtend einzustufen, bei deren Verletzung ein Bußgeld droht. Durch den Verweis auf § 8a Abs. 1 S. 2 BSIG in § 8a Abs. 1a S. 4 BSIG-E ist der Stand der Technik Maßstab bei der Wahl

[2] Referentenentwurf, S. 67, 68.
[3] Referentenentwurf, S. 68.
[4] Referentenentwurf, S. 68.
[5] Referentenentwurf, S. 68.

der Mittel der Angriffserkennung. Nach dem Stand der Technik bedeuten „Verfahren der künstlichen Intelligenz" aber unter Umständen mehr Risiko als Sicherheitsgewinn, weil diese Technologie, so man sie als solches bezeichnen kann, weder klar umrissen, unzureichend entwickelt und in der Regel nur kleine Bereiche abdecken kann. Es ist zweifelhaft, dass diese je die Angriffserkennung, Bedrohungsidentifikation und -abwehr, wie es § 8b Abs. 1a BSIG-E vorsieht, abdecken kann. Vielmehr dürfte der Einsatz von „KI" „nach dem Stand der Technik" dem Gesetzeszweck zuwiderlaufen.

Die Fatalität des Setzens auf sog. künstliche Intelligenz beschreiben *Yampolskiy* und *Spellchecker* wie folgt:

> *„however for general AI, failures have a fundamentally different impact. A single failure of a superintelligent system may cause a catastrophic event without a chance for recovery. The goal of cybersecurity is to reduce the number of successful attacks on the system; the goal of AI Safety is to make sure zero attacks succeed in bypassing the safety mechanisms. Unfortunately, such a level of performance is unachievable. Every security system will eventually fail; there is no such thing as a 100% secure system."*[6]

Ähnliches hat das BSI im Juli 2020 festgestellt:

> *„Based on this and the observation that adaptive attackers may circumvent any single published AI-specific defense to date, the article concludes that single protective measures are not sufficient but rather multiple measures on different levels have to be combined to achieve a minimum level of IT security for AI applications."*[7]

Von Unternehmen kann nichts Unmögliches gefordert werden. Feigenblattmaßnahmen als Konsequenz der Androhung eines empfindlichen Bußgelds sind inakzeptabel und gefährden die Ziele des Gesetzes. Nicht zuletzt könnte eine verständige Weigerung als Vorsatz verstanden und sanktionsverschärfend berücksichtigt werden.

Die Verpflichtungs- und korrespondierende Bußgeldvorschrift sollten gestrichen werden. Zu Wahl, Kombination und Einsatz von Systemen zur Angriffserkennung, Bedrohungsidentifikation und -abwehr sowie ggf. Schadensreduktion kann das BSI beraten und informieren (§ 3 Abs. 1 S. 2 Nr. 14 BSIG-E).

3. Wann Warnungen unter Namensnennung erfolgen können ist unklar

Bedenklich ist nicht zuletzt die neue Vorschrift des § 7 Abs. 2 S. 1 BSIG-E:

> *„Zur Erfüllung seiner Aufgaben nach § 3 Absatz 1 Satz 2 Nummer 14 und Nummer 14a kann das Bundesamt die Öffentlichkeit unter Nennung der Bezeichnung und des Herstellers des betroffenen Produkts vor Sicherheitslücken in informationstechnischen Produkten und Diensten und vor Schadprogrammen warnen, wenn hinreichende Anhaltspunkte dafür vorliegen, dass Gefahren für die Sicherheit in der Informationstechnik hiervon ausgehen, oder Sicherheitsmaßnahmen sowie den Einsatz bestimmter informationstechnischer Produkte und Dienste empfehlen."*

Grundsätzlich ist, ähnlich wie im Bereich der Produktsicherheit, die Information und Warnung der Öffentlichkeit zu begrüßen. Die vorstehende Vorgehensweise dürfte jedoch verfassungsrechtlich problematisch sein. Um ein Herstellerunternehmen an den öffentlichen Pranger zu stellen ist hiernach lediglich eine Gefahr für die Sicherheit in der Informationstechnik ausreichend.

---

[6] *Yampolskiy Spellchecker*, Artificial Intelligence Safety and Cybersecurity: a Timeline of AI Failures, 2015, https://arxiv.org/pdf/1610.07997.pdf.
[7] *Berghoff/Neu/von Twickel*, BSI, Vulnerabilities of Connectionist AI Applications: Evaluation and Defense, Juli 2020, https://www.frontiersin.org/articles/10.3389/fdata.2020.00023/full.

Welche Art von Gefahr, oder welcher Grad der Gefährdung eine solche schwerwiegende Maßnahme auslösen kann, ist unklar. Für die Annahme der nicht näher bezeichneten Gefahr genügen nicht zuletzt nur hinreichende Anhaltspunkte. Dieser Maßstab ist in doppelter Hinsicht unzureichend und steht in keinem Verhältnis zu den Folgen, die ein namentlich genanntes Herstellerunternehmen im Falle öffentlicher Warnung treffen können.

II. Die Stichprobe spricht für die Notwendigkeit vertiefter Prüfungen

Wie eingangs angesprochen ist es nicht möglich, ausführlicher auf Unzulänglichkeiten im Gesetzesentwurf einzugehen. Es sollte jedoch verdeutlicht worden sein, dass der Entwurf v.a. an Bestimmtheitsmängeln leidet, wobei Adressaten und Verpflichtungen unklar sowie sie flankierende Sanktionen scharf sind.

Es wird angeregt, dem Konsultations- und Gesetzgebungsprozess die notwendige Zeit einzuräumen, um verfassungsrechtlichen Anforderungen zu genügen.