21. Wahlperiode

Deutscher Bundestag
Innenausschuss

Ausschussdrucksache 21(4)062 C
vom 10. Oktober 2025

Schriftliche Stellungnahme

von Prof. Dr. Meinhard Schröder, Universität Passau vom 10. Oktober 2025

Öffentliche Anhörung

Gesetzentwurf der Bundesregierung

Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung

BT-Drucksache 21/1501

Prof. Dr. Meinhard Schröder

Lehrstuhl für Öffentliches Recht, Europarecht
und Informationstechnologierecht

UNIVERSITÄT PASSAU
Juristische Fakultät

Deutscher Bundestag
Innenausschuss
Herrn Vorsitzenden
Josef Oster MdB

- per Email -

Telefon | Prof. Dr. Meinhard Schröder
0851 509-2381
Telefax | 0851 509-2382
E-Mail | Meinhard.Schroeder
@uni-passau.de

Datum | 10.10.2025

Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (BT-Drucksache 21/1501)

Sehr geehrter Herr Vorsitzender,

als Anlage übersende ich die erbetene Stellungnahme zum o.g. Gesetzentwurf. Aufgrund der kurzfristigen Anfrage und anderweitiger Verpflichtungen konnte ich nur zu ausgewählten Punkten Stellung nehmen. Fragen beantworte ich gerne in der Sitzung.

Mit freundlichen Grüßen

Besucheradresse | Innstraße 39, Raum 114
Internetadresse | www.uni-passau.de/schroeder

Stellungnahme zum

Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung

(BT-Drucksache 21/1501)

Prof. Dr. Meinhard Schröder

Universität Passau, Passau Institute of Digital Security (PIDS)

Vorbemerkung

Die Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148, im Folgenden: **NIS-2-RL**, hätte bis zum 17. Oktober 2024 umgesetzt werden müssen (Art. 41 Abs. 1 NIS-2-RL). Dass die Umsetzung bisher nicht erfolgt ist, stellt nicht nur einen offensichtlichen Verstoß gegen europarechtliche Pflichten dar, der bereits ein Vertragsverletzungsverfahren nach sich zieht,[1] welches mit Strafzahlungen gem. Art. 260 Abs. 2 AEUV enden kann, sondern gefährdet zudem die IT-Sicherheit in den betroffenen Sektoren, wenn die zukünftig Normunterworfenen nicht schon jetzt freiwillig[2] entsprechende Maßnahmen ergreifen. Da bereits ein Vertragsverletzungsverfahren gegen Deutschland läuft, ist eine **vollständige und korrekte Umsetzung** besonders wichtig, denn es ist anzunehmen, dass die Kommission auf etwaige Fehler nicht mit einem neuen Vertragsverletzungsverfahren reagieren würde, sondern insoweit das laufende Verfahren in seinem schon fortgeschrittenen Stadium fortführen würde.

Die korrekte Umsetzung einer Richtlinie erfordert eine **Regelung durch Außenrechtssatz** (Parlamentsgesetz, Rechtsverordnung, Satzung), um den durch den EuGH etablierten Anforderungen an die Publizität, Klarheit und Bestimmtheit des Umsetzungsakts zu genügen.[3] Mittels Verwaltungsvorschriften, die bloßes „Innenrecht der Verwaltung“ darstellen, kann eine korrekte Richtlinienumsetzung nicht erfolgen.

Aus juristischer Perspektive sind zu dem vorliegenden Entwurf folgende Hinweise veranlasst:

1. Sprachliche Divergenzen

Die von der Richtlinie abweichende Terminologie (Art. 3 NIS-2-RL: wichtige und wesentliche Einrichtungen, BSIG-E: wichtige und besonders wichtige Einrichtungen) ist für die Normunterworfenen potentiell verwirrend, beispielsweise bei der Frage einer richtlinienkonformen Auslegung. Sie hindert aber nicht die vollständige Umsetzung. Generell ist zu empfehlen, wenn bestimmte tradierte Begriffe beibe-

[1] Siehe die Pressemitteilung der Europäischen Kommission, abrufbar unter https://germany.representation.ec.europa.eu/news/vertragsverletzungsverfahren-zwei-entscheidungen-zu-deutschland-2025-05-07_de.
[2] Die Richtlinie kann gegenüber Privaten keine unmittelbare belastende Wirkung entfalten, vgl. dazu *Ruffert*, in: Calliess/Ruffert, EUV/AEUV, Art. 288 Rn. 58 ff. m.w.N. aus der Rechtsprechung des EuGH.
[3] *Ruffert*, in: Calliess/Ruffert, EUV/AEUV, Art. 288 Rn. 33 ff. m.w.N. aus der Rechtsprechung des EuGH.

halten werden sollen, schon im europäischen Gesetzgebungsverfahren der deutschen Sprachfassung mehr Beachtung zu schenken, um Inkohärenzen zu vermeiden.

2. Geltung für die Bundesverwaltung (§ 29 BSIG-E)

Der Gesetzentwurf behandelt die Bundesverwaltung in § 29 BSIG-E anders als andere wichtige oder besonders wichtige Einrichtungen i.S.d. § 28 BSIG-E. Zwar werden Einrichtungen der Bundesverwaltung in § 29 Abs. 2 BSIG-E im Grundsatz den für besonders wichtige Einrichtungen geltenden Regelungen unterworfen. Hiervon sieht der Entwurf sodann aber zahlreiche Ausnahmen vor:

- Gem. § 29 Abs. 2 S. 1 BSIG-E gelten § 38, § 40 Abs. 3, § 61 und § 65 BSIG-E für keine der genannten Einrichtungen.
- Gem. § 29 Abs. 2 S. 2 BSIG-E gilt § 30 BSIG-E nicht für Einrichtungen der Bundesverwaltung, abgesehen vom Bundeskanzleramt und den Bundesministerien (und auch für diese nur vorbehaltlich der weiteren Ausnahme in Abs. 3).
- Gem. § 29 Abs. 3 gelten für die Geschäftsbereiche des Auswärtigen Amts und des Bundesministeriums der Verteidigung sowie den Bundesnachrichtendienst und das Bundesamt für Verfassungsschutz zusätzlich zu den Regelungen gemäß § 29 Abs. 2 BSIG-E auch nicht § 7 Abs. 5 Satz 4, § 10, § 13 Abs. 1 Nr. 1 lit. e) sowie §§ 30, 33 und 35 BSIG-E. Für BND und BfV ist das hinsichtlich § 30 BSIG-E eine redaktionelle Doppelung der Ausnahme; außerdem wird (wohl ein Tippfehler) § 13 doppelt erwähnt.

Die Regelung steht **nicht vollständig mit den Vorgaben der NIS-2-RL in Einklang**.

a) Definition der Bundesverwaltung (§ 29 Abs. 1 BSIG-E)

Art. 2 Abs. 2 lit. f) i.v.m. Anhang I NIS-2-RL räumt den Mitgliedstaaten eine gewisse **Definitionsbefugnis** im Bereich der Einrichtungen der öffentlichen Verwaltung ein. Worauf sich diese bezieht, ist aber nicht klar: Unter Berücksichtigung der englischen Sprachfassung liegt nahe, dass es vor allem um die Abgrenzung von zentraler, in Deutschland also Bundes-Verwaltung und regionaler Verwaltung, in Deutschland also Landesverwaltung geht. Vertretbar erscheint aber auch die Annahme, dass innerhalb der jeweiligen Ebene eine gewisse Auswahl der erfassten Einrichtungen zulässig bleibt. Die Definitionsbefugnis kann aber nicht so weit gehen, die Zuordnung völlig frei vorzunehmen. Zu berücksichtigen ist einerseits, dass Art. 6 Nr. 35 NIS-2-RL eine verbindliche Legaldefinition liefert, und dass sich andererseits aus der Zusammenschau von Art. 2 Abs. 2 lit. f) und Art. 2 Abs. 5 NIS-2-RL ein klares Stufenverhältnis ergibt, nach dem Einrichtungen der Verwaltung der Zentralregierung stets, auf regionaler Ebene nur bei besonderen Gefahren und auf lokaler Ebene freiwillig in den Geltungsbereich der Richtlinie einbezogen werden. Zentrale Bereiche der Bundesverwaltung vom Anwendungsbereich auszuschließen, ist damit kaum vereinbar. Dem Umsetzungsgesetz müssen bei teleologischer Betrachtung nicht nur die **Ministerien**, sondern auch die **unmittelbare Bundesverwaltung** unterfallen, soweit sie die Definition des Art. 2 Abs. 5 NIS-2-RL erfüllt. Jenseits dessen greift die Definitionsbefugnis des nationalen Gesetzgebers, was den Ausschluss der Sozialversicherungsträger und die fallweise Einbeziehung anderer juristischer Personen des öffentlichen Rechts deckt. Insgesamt bestehen daher gegen § 29 Abs. 1 BSIG-E keine Bedenken.

Hinzuweisen ist ergänzend darauf, dass von der Legaldefinition in § 29 Abs. 1 BSIG-E möglicherweise auch Justiz und Parlament bei machen Aufgaben erfasst sind, trotz der in Art. 6 Nr. 35 NIS-2-RL implizit vorgesehenen Möglichkeit, diese (wie die Zentralbank) auszunehmen. Eine solche Lesart überzeugt mit Blick auf das hohe Sicherheitsbedürfnis der genannten Einrichtungen, mag aber Fragen im Hinblick auf Gewaltenteilung und Unabhängigkeit aufwerfen.

b) Generelle Unanwendbarkeit bestimmter Vorschriften (§ 29 Abs. 2 S. 1 BSIG-E)

Die Anordnung der Unanwendbarkeit von § 38, § 40 Abs. 3, § 61 und § 65 BSIG-E steht nicht vollständig mit der NIS-2-RL in Einklang.

- § 38 BSIG-E dient ausweislich der Gesetzbegründung der Umsetzung von Art. 20 NIS-2-RL. Dieser lässt zwar „die nationalen Rechtsvorschriften in Bezug auf die für die öffentlichen Einrichtungen geltenden Haftungsregelungen sowie die Haftung von öffentlichen Bediensteten und gewählten oder ernannten Amtsträgern unberührt“; die von der Richtlinie angestrebte Governance und die Haftung sind aber zwei unterschiedliche Fragen. **Es ist daher zu empfehlen, den Verweis auf § 38 in § 29 Abs. 2 BSIG-E zu streichen**.
- § 40 Abs. 3 BSIG-E regelt Pflichten des BSI im Kontext seiner Rolle als zentrale Meldestelle. Diese werden soweit ersichtlich in der NIS-2-RL nicht genau vorgegeben, daher stellt die Ausnahme keinen Verstoß gegen die Pflicht zur Umsetzung der Richtlinie dar.
- § 61 BSIG-E regelt die Durchsetzungsbefugnisse des BSI gegenüber besonders wichtigen Einrichtungen. Die NIS-2-RL sieht in Art. 32 punktuelle Ausnahmen für die Durchsetzungsbefugnisse gegenüber Einrichtungen der Verwaltung vor (insbes. Art. 32 Abs. 5 UAbs. 3 NIS-2-RL); hinzu kommt eine generelle Befugnis der Mitgliedstaaten, zu entscheiden, „ob diesen Einrichtungen im Einklang mit den nationalen rechtlichen und institutionellen Rahmenbedingungen geeignete, verhältnismäßige und wirksame Aufsichts- und Durchsetzungsmaßnahmen auferlegt werden“ (Art. 31 Abs. 4 NIS-2-RL). Damit dürfte die vollständige Ausnahme vereinbar sein.
- § 65 BSIG-E enthält Bußgeldvorschriften. Die Ausnahme ist ohne Weiteres von Art. 34 Abs. 7 NIS-2-RL gedeckt.

c) Unanwendbarkeit von § 30 BSIG-E (§ 29 Abs. 2 S. 2 BSIG-E)

Gem. § 29 Abs. 2 S. 2 BSIG-E gilt § 30 BSIG-E nicht für Einrichtungen der Bundesverwaltung abgesehen vom Bundeskanzleramt und den Bundesministerien. Mit anderen Worten besteht nur für Bundeskanzleramt und Bundesministerien eine Pflicht zum Risikomanagement gem. § 30 BSIG-E. Die Vorschrift setzt **Art. 21 NIS-2-RL** um, der **keine Ausnahmen für Einrichtungen der öffentlichen Verwaltung** enthält. Erforderlich ist daher eine anderweitige Umsetzung der Vorgaben des Art. 21 NIS-2-RL Diese erfolgt nach dem Willen des Gesetzgebers in **Art. 44 BSIG-E**.

Ob die Vorgaben des BSI, auf die § 44 Abs. 1 und 2 BSIG-E Bezug nimmt, in materieller Hinsicht alle Anforderungen des Art. 21 NIS-2-RL erfüllen, wie § 44 Abs. 3 S. 1 BSIG-E im Wege einer Fiktion behauptet, kann hier nicht im Detail untersucht werden. Höchst problematisch erscheint aber, dass weite Teile der Bundesverwaltung nur den Vorgaben des § 44 Abs. 1 BSIG-E unterliegen und nicht einmal

den IT-Grundschutzkatalog des BSI, sondern nur ein von ihnen selbst im Rahmen des Benehmens mit dem BSI zu beeinflussendes Sicherheitsniveau einhalten müssen. Damit werden die Anforderungen das durch § 30 BSIG-E geforderten Sicherheitsniveaus nicht erreicht, was der Entwurf auch anerkennt, indem er in § 44 Abs. 3 Satz 1 BSI-G nur die kumulative Erfüllung der Anforderungen aus § 44 Abs. 1 und 2 für eine Äquivalenz ausreichen lässt. Dies stellt **keine ordnungsgemäße Umsetzung der NIS-2-RL** dar und lässt sich auch nicht mit der Behauptung rechtfertigen, die Bundesverwaltung außer Bundeskanzleramt und Ministerien sei durch diese gar nicht betroffen und nur im Wege der überschießenden Richtlinienumsetzung einbezogen (s.o. unter a)). Bedenken bestehen außerdem in formeller Hinsicht wegen des Erfordernisses der Richtlinienumsetzung durch verbindliche Außenrechtssätze (siehe Vorbemerkung), die formal zwar eingehalten wird, aber durch die Verweise letztlich doch die zentralen inhaltlichen Fragen dem Soft Law des BSI überlässt.

Weiter liegt die Frage auf der Hand, warum die Beachtung der Anforderungen aus § 44 Abs. 1 und 2, insbesondere des IT-Grundschutzkatalogs des BSI für „besonders wichtige Einrichtungen“ für Bundeskanzleramt und Ministerien ausreicht, um die Anforderungen der Richtlinie zu erfüllen, im nichtstaatlichen Bereich aber das Risikomanagement gem. § 30 BSIG-E verlangt wird. **Parallele Anforderungen** für öffentliche und private Stellen entsprechen nicht nur dem europäischen Regelungsansatz, sondern würden auch die **Akzeptanz der Regelung** stärken und der **Vorbildrolle der Verwaltung** im Bereich der IT-Sicherheit eher gerecht werden.

Schwer verständlich ist schließlich die Regelungsstruktur: Warum werden Bundeskanzleramt und Ministerien in § 29 Abs. 2 Satz 2 BSIG-E überhaupt formal an § 30 BSIG gebunden, wenn sie wegen § 44 Abs. 3 Satz 1 BSI-G in Wahrheit stattdessen die Erfüllung der Anforderungen aus § 44 Abs. 1 und 2 BSIG-E erfüllen werden (und dies auch müssen)? Dass Bundeskanzleramt und Bundesministerien ein „förmliches“ Risikomanagement gem. § 30 BSIG-E neben den Verpflichtungen aus § 44 Abs. 1 und 2 BSIG-E durchführen werden, erscheint jedenfalls fernliegend; auf gegebenenfalls zu beachtende tertiärrechtliche Vorgaben nimmt § 44 Abs. 3 BSIG-E selbst schon Bezug.

d) Unanwendbarkeit weiterer Vorschriften für einige Akteure (§ 29 Abs. 3 BSIG-E)

Gem. § 29 Abs. 3 BSIG-E gelten einige weitere Vorschriften des BSIG-E nicht für die Geschäftsbereiche des Auswärtigen Amts und des Bundesministeriums der Verteidigung sowie den Bundesnachrichtendienst und das Bundesamt für Verfassungsschutz. Insofern ist darauf hinzuweisen, dass gem. **Art. 2 Abs. 7 NIS-2-RL** diese für bestimmte Bereiche nicht gilt. Bundesministerium der Verteidigung, Bundesnachrichtendienst und Bundesamt für Verfassungsschutz fallen unzweifelhaft unter die Ausnahme „nationale Sicherheit, öffentliche Sicherheit, Verteidigung oder Strafverfolgung“. Für das Auswärtige Amt ist dies weniger klar, zumal Erwägungsgrund 8 der NIS-2-RL nur diplomatische und konsularische Vertretungen der Mitgliedstaaten in Drittländern sowie deren Netz- und Informationssysteme, sofern sich diese Systeme in den Räumlichkeiten der Mission befinden oder für Nutzer in einem Drittland betrieben werden, aus dem Anwendungsbereich ausnehmen möchte, nicht hingegen die „Zentrale“.

Davon ausgehend stellt sich die Einbeziehung der in § 29 Abs. 3 genannten Stellen in den Anwendungsbereich des BSIG-E weitgehend als **überschießende Richtlinienumsetzung** dar, die aber zur Gewährleistung eines hohen Niveaus an IT-Sicherheit sinnvoll erscheint. Es geht nicht darum, dass

die genannten Bereiche kein Bedürfnis nach IT-Sicherheit aufweisen würden – er ist lediglich nicht europarechtlich überformt. Für das wohl nicht vollständig von Art. 2 Abs. 7 NIS-2-RL erfasste **Auswärtige Amt** ergibt eine detailliertere Analyse der Ausnahmen Folgendes:

- § 7 Abs. 5 Satz 4 und § 10 BSIG-E regeln Anweisungsrechte des BSI gegenüber bestimmten Einrichtungen der Bundesverwaltung. Diese können gem. Art. 31 Abs. 4 NIS-2-RL ausgeschlossen werden (s.o.). Bei § 13 Abs. 1 Nr. 1 lit. e) stellt sich die Frage, ob die Befugnis des BSI zu Warnungen und Informationen an die Öffentlichkeit oder an die betroffenen Kreise ebenfalls zu den Aufsichts- und Durchsetzungsmaßnahmen zählt. Verneint man dies, wäre der Verweis zu streichen, da die Vorschrift der Umsetzung von Art. 32 Abs. 4 lit. a und Art. 33 Abs. 4 NIS-2-RL dient und keine dieser Vorschriften Ausnahmen für die öffentliche Verwaltung vorsieht.
- § 33 BSIG-E regelt die Registrierungspflicht gegenüber dem BSI. Die Gesetzesbegründung sieht die Vorschrift als Umsetzung des Art. 3 Abs. 3 NIS-2-RL an. Dieser verpflichtet allerdings nur die Mitgliedstaaten, eine Liste zu erstellen, und schreibt nicht vor, wie die dafür erforderlichen Daten beschafft werden. Solange die Liste im Ergebnis korrekt erstellt wird, beeinträchtigt die Ausnahme die Richtlinienumsetzung nicht.
- § 35 BSIG-E regelt eine Befugnis des BSI, bei erheblichen Sicherheitsvorfällen Einrichtungen zu verpflichten, die Empfänger ihrer Dienste zu informieren. Die Vorschrift soll Art. 23 Abs. 2 NIS-2-RL umsetzen. Dieser verpflichtet die Mitgliedstaaten aber nur, sicherzustellen, dass die Dienstempfänger informiert werden, und verlangt nicht, dass das BSI hierzu Anweisungen erteilt. Die Ausnahme beeinträchtigt die Richtlinienumsetzung daher nicht, solange die Information der Dienstempfänger anderweitig „sichergestellt“ ist.

3. Untersagung des Einsatzes kritischer Komponenten (§ 41 BSIG-E)

Die Möglichkeit der Untersagung des Einsatzes kritischer Komponenten kann im Grundsatz der Erfüllung einer **grundrechtlichen Schutzpflicht** dienen, die aus dem Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG, im Folgenden: IT-System-Grundrecht) fließt.[4]

Bedenken bestehen allerdings mit Blick auf die **Vollzugsfähigkeit der Vorschrift**. § 41 BSIG-E enthält mehrere Verweise auf die in Art. 56 Abs. 4 BSIG genannten Ressorts (Bundesministerium für Wirtschaft und Energie, Bundesministerium der Finanzen, Bundesministerium der Justiz und für Verbraucherschutz, Bundesministerium für Arbeit und Soziales, Bundesministerium der Verteidigung, Bundesministerium für Landwirtschaft, Ernährung und Heimat, Bundesministerium für Gesundheit, Bundesministerium für Verkehr, Bundesministerium für Umwelt, Klimaschutz, Naturschutz und nukleare Sicherheit, Bundesministerium für Forschung, Technologie und Raumfahrt, Bundesministerium für Digitales und Staatsmodernisierung). Während das in § 41 Abs. 2 BSIG-E geforderte Benehmen, das nur eine Berücksichtigung der Stellungnahme der Ressorts durch das anordnungsbefugte Bundesministerium des Innern erfordert,[5] keine Probleme aufwirft, könnte das in Art. 41 Abs. 4 BSIG-E gefor-

[4] Vgl. zur parallelen Konstellation im Anwendungsbereich des Fernmeldegeheimnisses aus Art. 10 GG BVerfGE 158, 170.
[5] Zum Begriff vgl. BVerwGE 92, 258 (262); BVerwG, NVwZ 2001, 90 (91); *Simnacher*, BayVBl. 1983, 103 ff.

derte **Einvernehmen mit elf Ressorts**, die möglicherweise völlig unterschiedliche Interessen (beispielsweise günstige Preise von Dienstleistungen für Verbraucher) verfolgen, nur schwer erreichbar sein. Zwar ist es verfassungsrechtlich sogar geboten, dass die (faktische) Anordnung der nachträglichen Entfernung kritischer Komponenten höheren Anforderungen unterliegt als die anfängliche Untersagung ihres Einsatzes, dies sollte sich aber in den materiellen Voraussetzungen widerspiegeln, die die IT-Sicherheit gegen andere Verfassungsgüter abwägen, und nicht in einer potentiell dysfunktionalen prozeduralen Ausgestaltung der Vorschrift.

Zu empfehlen ist weiter, den **Begriff der öffentlichen Ordnung in § 41 BSIG-E zu streichen**. Mit dem Begriff gemeint sind nach gängiger Auffassung „die ungeschriebenen Regeln, deren Beachtung nach den herrschenden Anschauungen als unerlässliche Voraussetzung eines geordneten Zusammenlebens angesehen wird“[6]. Ihm kommt im Sicherheitsrecht nur geringe praktische Bedeutung zu und es wird teilweise sogar für verfassungswidrig gehalten, zum Schutz der (nicht durch den Gesetzgeber verrechtlichten) öffentlichen Ordnung Grundrechtseingriffe vorzunehmen.[7] Jedenfalls können Maßnahmen von erheblicher grundrechtlicher Eingriffsintensität wie die Untersagung des Einsatzes kritischer Komponenten wohl nicht auf eine bloße Beeinträchtigung der öffentlichen Ordnung gestützt werden. Angesichts der Reichweite des Begriffs der öffentlichen Sicherheit, der nach gängiger Auffassung die Unversehrtheit der Rechtsgüter des Einzelnen, des Staates und seiner Einrichtungen sowie der Rechtsordnung als solcher umfasst,[8] besteht für einen Rekurs auf den Begriff der öffentlichen Ordnung auch kein Bedürfnis.

Zu erinnern ist schließlich daran, dass insbesondere § 41 Abs. 2 Satz 2 Nr. 1 und 3 die Tür zu einer **politischen Entscheidung** relativ weit öffnet. Es geht hier nicht mehr um die Bekämpfung technischer Sicherheitsrisiken, die sich oft auch erst im Nachhinein erkennen lassen, sondern um vorsorgliche Maßnahmen aufgrund der befürchteten Kompromittierung von allen vorstellbaren IKT-Komponenten, die in einer kritischen Umgebung genutzt werden. Nach welchen Kriterien hier ausgewählt werden soll, erscheint schwer vorhersehbar.

4. Schwachstellenmanagement (§§ 15 Abs. 2, 43 Abs. 5 BSIG-E)

Für die IT-Sicherheit stellen Schwachstellen, insbesondere sog. Zero-Day-Schwachstellen, die der Hersteller der Hardware oder Software nicht kennt und deshalb auch nicht beheben kann, eine besondere Bedrohung dar. Die **staatliche Schutzpflicht**, die u.a. aus dem IT-System-Grundrecht fließt (s.o.), streitet hier dafür, dass Behörden, die Kenntnis von solchen Schwachstellen erlangen, diese dem Hersteller melden müssen, damit sie geschlossen werden und nicht durch Dritte ausgenutzt werden können. Andererseits haben staatliche Stellen möglicherweise ein Eigeninteresse daran, Sicherheitslücken zur Gefahrenabwehr, Aufklärung usw. zu nutzen, und verfolgen dabei ebenfalls Ziele von Verfassungsrang.

In dieser Situation verlangt das Bundesverfassungsgericht vom Gesetzgeber „eine Regelung zur grundrechtskonformen **Auflösung des Zielkonflikts** zwischen dem Schutz informationstechnischer

---

[6] Vgl. etwa *Möstl*, in: BeckOK PolR Bayern, Systematische und begriffliche Vorbemerkungen zum Polizeirecht in Deutschland, Rn. 14.
[7] *Bäcker*, in: Lisken/Denninger PolR-HdB, Abschnitt D. Rn. 73.
[8] Vgl. etwa *Möstl*, in: BeckOK PolR Bayern, Systematische und begriffliche Vorbemerkungen zum Polizeirecht in Deutschland, Rn. 7.

Systeme vor Angriffen Dritter mittels unbekannter Sicherheitslücken einerseits und der Offenhaltung solcher Lücken zur Ermöglichung einer der Gefahrenabwehr dienenden Quellen-Telekommunikationsüberwachung andererseits“.[9] Für die Ausgestaltung der Regelung hat das Bundesverfassungsgericht genauere Vorgaben entwickelt: „Der Behörde muss eine Abwägung der gegenläufigen Belange für den Fall aufgegeben werden, dass ihr eine Zero-Day-Schutzlücke bekannt wird. Es ist sicherzustellen, dass die Behörde bei jeder Entscheidung über ein Offenhalten einer unerkannten Sicherheitslücke einerseits die Gefahr einer weiteren Verbreitung der Kenntnis von dieser Sicherheitslücke ermittelt und andererseits den Nutzen möglicher behördlicher Infiltrationen mittels dieser Lücke quantitativ und qualitativ bestimmt, beides zueinander ins Verhältnis setzt und die Sicherheitslücke an den Hersteller meldet, wenn nicht das Interesse an der Offenhaltung der Lücke überwiegt.“[10] Nach welchen Kriterien diese vorzunehmen ist, lässt das Bundesverfassungsgericht offen. Fraglich ist auch, ob alle Behörden diese Abwägung leisten können.

Der vorliegende Entwurf regelt den Umgang mit Schwachstellen in verschiedenen Vorschriften. **§ 15 Abs. 2 BSIG-E** verpflichtet das BSI dazu, den für ein System Verantwortlichen zu informieren, wenn es im Rahmen der ihm aufgegebenen Angriffsdetektion bekannte Schwachstellen oder andere Sicherheitsrisiken entdeckt. Insofern wird die Schutzpflicht jedenfalls erfüllt, allerdings geht es in der Vorschrift nicht um Zero-Day-Schwachstellen.

Nicht geregelt ist weiter die Situation, dass das BSI auf anderem Weg von Schwachstellen Kenntnis erlangt, etwa durch Whistleblower. Hier **fehlt es an einer hinreichenden gesetzlichen Regelung**. Für das BSI greift auch nicht § 43 Abs. 5 BSIG-E, der das BSI als Empfänger einer möglichen Unterrichtung nennt und damit nicht gleichzeitig verpflichtet, obwohl es selbst auch unter den Begriff „Einrichtung der Bundesverwaltung“ subsumiert werden könnte. Insofern wird der durch das Bundesverfassungsgericht erteilte Regelungsauftrag nicht erfüllt, wenn man nicht – angesichts der ausdifferenzierten Regelungsstruktur wenig überzeugend – § 15 Abs. 2 BSIG-E als Ausdruck einer generellen Pflicht des BSI ansieht, Systemverantwortliche stets über Schwachstellen zu informieren. Zur Erfüllung der Schutzpflicht beitragen könnte auch eine Regelung der **Straflosigkeit von sog. White Hat Hackern**, die das BSI über Schwachstellen informieren; die weite Formulierung der §§ 202a ff. StGB stellt hier ein Hindernis dar.

Der Gesetzgeber kann das BSI mit der verfassungsrechtlich gebotenen Abwägungsentscheidung betrauen; eine dezentrale Entscheidung durch diejenige staatliche Stelle, die Kenntnis von einer Schwachstelle erlangt, ist aber auch zulässig. Dem entspricht im Grundsatz die Regelung des § 43 Abs. 5 BSIG-E, der in Satz 1 allen Stellen der Bundesverwaltung eine **grundsätzliche Pflicht, das BSI zu unterrichten,** auferlegt – hier trifft dann das BSI die Entscheidung, wie weiter zu verfahren ist, wofür allerdings die gesetzlichen Maßstäbe fehlen (s.o.).

Soweit von der Unterrichtungspflicht Ausnahmen gem. (§ 43 Abs. 5 Satz 1 a.E. oder § 43 Abs. 5 Satz 2 BSIG-E bestehen, verbleibt die **Abwägungsentscheidung bei der Behörde, die die Sicherheitslücke entdeckt hat**. Die von der Unterrichtungspflicht ausgenommenen Behörden müssen daher fachlich in der Lage sein, die Abwägungsentscheidung selbst zu treffen. Allerdings bringt das Gesetz nicht einmal hinreichend klar zum Ausdruck, dass eine Abwägungsentscheidung erforderlich ist. Zwar lässt sich § 43 Abs. 5 Satz 2 BSIG-E wohl dahingehend interpretieren, dass eine Meldung an

[9] BVerfGE 158, 170 Ls. 2 b).
[10] BVerfGE 158, 170 (189 f. Rn 44.)

das BSI möglich bleibt und lediglich keine Pflicht besteht, sodass die vom Bundesverfassungsgericht geforderte Abwägung stattfinden Es besteht aber die Gefahr, dass die Vorschrift so interpretiert wird, dass in den vorgesehenen Fällen die Meldung stets unterbleiben darf. Eine **Klarstellung** dahingehend, dass im Einzelfall abgewogen werden muss, ist daher zu empfehlen, insbesondere weil das Bundesverfassungsgericht an die Normenklarheit im Bereich des (IT-)Sicherheitsrechts hohe Anforderungen stellt und vom Gesetzgeber verlangt, der Exekutive sehr detaillierte Handlungsvorgaben zu machen.[11]

5. Nachweisfrist (§ 43 Abs. 1 BSIG-E)

Die Nachweisfrist von 5 Jahren erscheint aus der Perspektive des Europarechts bedenklich. Deutschland hätte seit 18. Oktober 2024 die Vorschriften, mit denen es die NIS-2-RL umsetzt, anwenden müssen. Die in Richtlinien ungewöhnliche Vorgabe des Art. 41 Abs. 1 UAbs. 2 NIS-2-RL zeigt, wie wichtig dem Unionsgesetzgeber das Anliegen der IT-Sicherheit ist. Um „sicherzustellen“ (so die wiederkehrende Formulierung der Richtlinie), dass die wichtigen und besonders wichtigen Einrichtungen ab dem 18. Oktober 2024 das europarechtlich gewünschte Sicherheitsniveau aufweisen, darf § 43 Abs. 1 nicht als Übergangsfrist verstanden werden, sondern nur als Frist für den formalen Nachweis. Die materiellen Vorgaben sind **unverzüglich zu erfüllen**, was auch im Gesetz klargestellt werden könnte.

6. Amt des Koordinators für Informationssicherheit (§ 48 BSIG-E)

Die Rolle des Koordinators für Informationssicherheit ist völlig unklar. Auch die Gesetzesbegründung liefert insofern keine Erläuterung. Dem Koordinator werden im Gesetzentwurf auch weder Aufgaben noch Befugnisse zugewiesen. Hier sollte das Gesetz eine Klärung vornehmen; alternativ könnte die Vorschrift gestrichen werden – einen Koordinator kann die Bundesregierung auch ohne gesetzliche Grundlage bestellen.

Passau, den 10. Oktober 2025

gez. Prof. Dr. Meinhard Schröder

[11] *Schröder*, in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, 3. Aufl. 2026, Vorbem. § 19 BNDG Rn. 5 (i.E.).