21. Wahlperiode

Deutscher Bundestag
Innenausschuss

Ausschussdrucksache 21(4)062 A
vom 9. Oktober 2025

Schriftliche Stellungnahme

von Dr. Sven Herpig, interface vom 8. 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

Stellungnahme von Dr. Sven Herpig, Lead Cybersecurity Policy and Resilience bei interface – Tech analysis and policy ideas for Europe e.V. (ehemals: Stiftung Neue Verantwortung), für die öffentliche Anhörung des Innenausschusses des Deutschen Bundestags am 13. Oktober 2025 zum 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)

Kontakt

Dr. Sven Herpig
Lead Cybersecurity Policy and Resilience
interface – Tech analysis and policy ideas for Europe e.V.
Email: sherpig@interface-eu.org
Mastodon: @z_edian@infosec.exchange

interface

Inhaltsverzeichnis

1. Vorbemerkung

Beim NIS-2-Umsetzungsgesetz handelt es sich um die nationale Transposition der zweiten EU-Richtlinie über die Sicherheit von Netzen und Informationssystemen (NIS-2-Richtlinie). Das NIS-2-Umsetzungsgesetz steht verspätet am Ende eines langwierigen Aushandlungsprozesses, erst auf europäischer und dann auf deutscher Ebene. Die in der Europäischen Union vereinbarten Anforderungen, die unter anderem auf der prekären Gefährdungslage basieren, treffen so auf die nationalen gesetzlichen Grenzen, die zum Beispiel vom Grundgesetz vorgegeben sind.

Während die Notwendigkeit für so ein Gesetzgebungsvorhaben hinreichend klar ist, sollte nicht davon ausgegangen werden, dass diese Gesetzesänderungen an sich mehr IT-Sicherheit in und für Deutschland schaffen. IT-Sicherheitsprüfungen und mögliche Bußgelder schaffen weitere Anreize für die Betreiber der IT-Infrastrukturen im Geltungsbereich, für mehr IT-Sicherheit zu sorgen. Die Wahrscheinlichkeit von Prüfungen und damit verbundenen möglichen Bußgeldern bedeutet für die betroffenen Unternehmen im Zweifelsfall eine finanzielle Abwägung. Es gilt daher, auch außerhalb des reinen Gesetzgebungsvorhabens, positive Anreize für Unternehmen zu schaffen, damit diese die notwendigen IT-Sicherheitsanforderungen erfüllen. Dazu gehören unter anderem einfache, unbürokratische Verfahren, sowie reziproke, handlungsbefähigende Kommunikation zwischen Behörden und Betreibern von IT-Infrastrukturen im Geltungsbereich, zum Beispiel beim Meldeportal[1]. Zusätzlich sollte die Bundesregierung ein Maßnahmenpaket erarbeiten, das das Ziel hat, kurzfristig (<3 Jahre) die benötigten Fachkräfte, zum Beispiel durch Umschulungen und Ausbildungen, dem Arbeitsmarkt zur Verfügung zu stellen. Denn aktuell ist vollkommen unklar, wer die mehreren hundert benötigten Planstellen für die Umsetzung des Gesetzgebungsvorhabens bei den Behörden besetzen soll – ganz zu schweigen von den Fachkräften, die die Wirtschaft zur Umsetzung benötigen wird.

Die Verabschiedung des, wie auch immer im Detail lautenden, NIS-2-Umsetzungsgesetz ist nicht das Ende eines umfassenden Vorhabens für mehr

[1] Nationaler Normenkontrollrat (2024): NKR-Stellungnahme Nr. 6824 Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (BMI)

IT-Sicherheit, sondern gerade mal ihr Anfang. Die wirkliche Erhöhung der IT-Sicherheit findet dann durch die Implementierung statt, die noch weit über diese Legislaturperiode hinausgehen wird.

2. Empfehlungen

Es werden im Folgenden Anpassungen zum “Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung” (BT-Drucksache 21/1501) angeregt. Die Empfehlungen erfolgen aus inhaltlicher, nicht aus rechtlicher Betrachtung.

IT-Sicherheit für Bund und Länder

Bezug unter anderem auf § 3 Absatz 1 Sätze 18 und 20 BSIG-E sowie § 4 Absätze 1 und 2 BSIG-E.

Der Bundesrechnungshof bescheinigt der Bundesregierung, dass sie „die Cybersicherheitsstrategie neu ausrichten [muss ..] und die Cybersicherheitsarchitektur reformieren [muss]”.[2] Während es bisher verpasst wurde eine Cybersicherheitsarchitektur[3] für Bund und Länder oder eine Cybersicherheitsstrategie für Bund und Länder zu schaffen wird mit dem vorliegenden Entwurf der Transposition der NIS-2-Richtlinie nun auch noch die Chance verpasst eine einheitlichere IT–Sicherheitsregulierung für Bund und Länder zu schaffen. Diese vertane Chance wirkt zum Beispiel mit Blick auf § 3 BSIG-E Absatz 1 Satz 20 geradezu bizarr. Mit dieser Befugnis kann das Bundesamt für Sicherheit in der Informationstechnik zwar Anwender beraten, informieren und warnen, aber nicht die Einrichtungen der Länderverwaltungen und Kommunen.

Neben den unten genannten Änderungsmöglichkeiten am § 3 BSIG-E könnte dies über eine entsprechende Änderung des Art 91c GG erreicht werden – was natürlich auch der Zustimmung von Teilen der Opposition bedarf. Es sollte nochmals geprüft werden, ob eine Ausweitung des Geltungsbereichs auf die Einrichtungen der Länderverwaltungen umsetzbar ist, da davon die IT-Sicherheit in Deutschland sehr wahrscheinlich profitieren würde. Und das sollte im Interesse aller Parteien liegen. Da diese Änderung vermutlich erst in einem nachfolgenden Gesetzgebungsvorhaben

[2] Bundesrechnungshof (2025): Bericht nach § 88 Absatz 2 BHO zur Cybersicherheit
[3] interface (2025): Cybersicherheitsarchitektur

realisiert werden kann, sollte sie im besten Fall gemeinsam mit einer Optimierung der Bund-Länder-Cybersicherheitsarchitektur, sowie der Verabschiedung einer Bund-Länder-Cybersicherheitsstrategie einhergehen.

Staatlicher Umgang mit Schwachstellen

Bezug unter anderem auf § 3 Absatz 1 Sätze 4 und 18 BSIG-E, § 4 Absatz 3 BSIG-E, § 6 BSIG-E, § 13 Absatz 1 Satz 2 BSIG-E, § 14 BSIG-E, und § 43 Absatz 5 BSIG-E.

Seit mehreren Legislaturperioden arbeiten Teile der Bundesregierung daraufhin, eine umfassende Regelung für den Umgang mit Schwachstellen zu finden. Der Sachverständige hat hierzu einen Vorschlag vorgelegt[4] und in einer Sachverständigenstellungnahme[5] eine mögliche Alternative skizziert. Der aktuelle Entwurf verzichtet leider weiterhin darauf, den Umgang mit Schwachstellen für IT-Sicherheits-, nachrichtendienstliche oder polizeiliche Zwecke durch die Bundes- und Landesbehörden klar zu regeln. Die diesbezüglichen Änderungen im BSIG-E tragen daher nur zur Fragmentierung und Rechtsunsicherheit bei, ohne einen umfassenden Ansatz zur Stärkung der IT-Sicherheit zu leisten.

Koordinator:in für Informationssicherheit

Bezug unter anderem auf § 48 BSIG-E.

Im Bericht nach § 88 Absatz 2 BHO zur Cybersicherheit des Bundesrechnungshofes aus dem Juli 2025 heißt es: „Die Informationstechnik (IT) des Bundes ist nicht bedarfsgerecht geschützt".[6] Hinzu kommt, dass größere Digitalisierungsprojekte der jüngeren Vergangenheit, wie zum Beispiel Bund-ID, digitaler Führerschein, ID Wallet oder elektronische Patientenakte, teils gravierende IT-Sicherheitsprobleme aufweisen.[7]

---

[4] Sven Herpig (2018): Schwachstellen-Management für mehr Sicherheit und Sven Herpig (2025): Vulnerability Disclosure: Guiding Governments from Norm to Action How to Implement Norm J of the United Nations Norms of Responsible State Behaviour in Cyberspace

[5] Sven Herpig (2023): Stellungnahme von Dr. Sven Herpig, Leiter für Cybersicherheitspolitik und Resilienz bei der Stiftung Neue Verantwortung e. V. (SNV), für die öffentliche Anhörung des Ausschusses für Digitales des Deutschen Bundestags am 25. Januar 2023 zum Thema "Cybersicherheit - Zuständigkeiten und Instrumente in der Bundesrepublik Deutschland".

[6] Bundesrechnungshof (2025): Bericht nach § 88 Absatz 2 BHO zur Cybersicherheit

[7] Verweise siehe Sven Herpig und Paul Zenker (2025): Bewährungsprobe fürs Digitalministerium: Von unsicherer Digitalisierung zu sicheren KI-Anwendungen

Dies macht die koodinierende Rolle für Informationssicherheit („CISO-Bund") unverzichtbar. Neben der Begleitung von Digitalisierungsprojekten und der entsprechenden Prüfung auf Einhaltung von IT-Sicherheitskriterien a priori, könnte ein Koordinator für Informationssicherheit[8] zum Beispiel auch Vorfälle a posteriori im Rahmen eines Cyber Safety Review Boards[9] aufarbeiten.

Damit die Rolle des CISO-Bund effektiv die IT-Sicherheit Deutschlands verbessern kann, müssen mehrere Voraussetzungen erfüllt sein. Im Rahmen von *Checks and Balances* und basierend auf anerkannten internationalen Best Practices und Standards muss die Rolle fachlich unabhängig von der zu prüfenden Rolle („CIO-Bund") sein. Neben einer ausreichenden Ressourcenausstattung, muss die Rolle CISO-Bund mit Prüfbefugnissen, Koordinierungsaufgabe zur Harmonisierung von IT-Sicherheitsstandards, sowie einem Vortragsrecht beim Vorgesetzten der Rolle CIO-Bund und regelmäßigen Berichterstattungen an Bundesrechnungshof oder Parlament ausgestattet werden.

Die Bundesregierung kann zeigen, wie ernst sie es mit der Absicherung der IT-Infrastrukturen der Bundesverwaltung und der IT-Projekte des Bundes meint, indem sie eine dedizierte CISO-Bund-Stelle schafft. Die Rolle sollte nicht einfach einer bestehenden Funktion, zum Beispiel P BSI, zugeordnet werden.

Änderungen an § 1 Satz 3 BSIG-E

Wortlaut: „Aufgaben gegenüber den Bundesministerien führt das Bundesamt auf Grundlage wissenschaftlich-technischer Erkenntnisse durch."

Empfehlung: „Seine Aufgaben führt das Bundesamt auf Grundlage wissenschaftlich-technischer Erkenntnisse durch."

Begründung: Es ist unklar, warum das Bundesamt seine Aufgaben gegenüber anderen Einrichtungen der Bundesverwaltung, Einrichtungen der Landesverwaltungen und Kommunen, Unternehmen, Verbraucher:innen und anderen nicht auf Grundlage

[8] Sven Herpig (2023): Stellungnahme von Dr. Sven Herpig, Leiter für Cybersicherheitspolitik und Resilienz bei der Stiftung Neue Verantwortung e. V. (SNV), für die öffentliche Anhörung des Ausschusses für Digitales des Deutschen Bundestags am 25. Januar 2023 zum Thema "Cybersicherheit - Zuständigkeiten und Instrumente in der Bundesrepublik Deutschland".
[9] Sven Herpig (2024): Cyber Safety Review for Webex-Vulnerability Handling?*

wissenschaftlich-technischer Erkenntnisse durchführen soll. Bestärkt wird die Empfehlung durch die in der NIS-2-Richtlinie geforderten „operativen Unabhängigkeit" der Implementierungsbehörde. Weiterführende Erklärungen finden sich in der Stellungnahme des Sachverständigen.[10]

Änderungen an § 2 Absatz 1 BSIG-E

Wortlaut: „„Beinahevorfall" ein Ereignis, das die Verfügbarkeit, Integrität oder Vertraulichkeit gespeicherter, übermittelter oder verarbeiteter Daten oder der Dienste, die über informationstechnische Systeme, Komponenten und Prozesse angeboten werden oder zugänglich sind, beeinträchtigt haben könnte, dessen Eintritt jedoch erfolgreich verhindert worden ist oder aus anderen Gründen nicht erfolgt ist;"

Empfehlung: Ersatzlos streichen, inklusiver aller Verweise, oder enger fassen.

Begründung: Es handelt sich hierbei um eine extrem weitgefasste Definition. Gerade im Zusammenhang mit §§ 5, 6 und 58 BSIG-E wird hier beim Bundesamt ein großer bürokratischer Mehraufwand ohne erkennbaren Mehrwert für die IT-Sicherheit geschaffen.

Änderungen an § 2 Absatz 23 BSIG-E

Wortlaut: „[...] bei denen Störungen der Verfügbarkeit, Integrität und Vertraulichkeit zu einem Ausfall oder zu einer erheblichen Beeinträchtigung [...]"

Empfehlung 1: „[...] bei denen Störungen der Verfügbarkeit, Integrität und/oder Vertraulichkeit zu einem Ausfall oder zu einer erheblichen Beeinträchtigung [...]"

Begründung 1: Die Verletzung einer oder mehrerer Schutzziele kann zu einem Ausfall oder einer erheblichen Beeinträchtigung führen.

Empfehlung 2: Erklärung, warum Authentizität als Schutzziel gestrichen wurde.

[10] Sven Herpig (2023): Stellungnahme von Dr. Sven Herpig, Leiter für Cybersicherheitspolitik und Resilienz bei der Stiftung Neue Verantwortung e. V. (SNV), für die öffentliche Anhörung des Ausschusses für Digitales des Deutschen Bundestags am 25. Januar 2023 zum Thema "Cybersicherheit - Zuständigkeiten und Instrumente in der Bundesrepublik Deutschland".

Begründung 2: Für die weitere Beurteilung ist es relevant zu wissen, ob Authentizität im Rahmen einer Rückbesinnung auf und Integration in die klassische CIA-Triade (Verfügbarkeit, Integrität und Vertraulichkeit) gestrichen wurde, oder ob es dafür eine inhaltliche Begründung gibt. Vergleiche zur Konsistenz zum Beispiel § 3 TKG-E und § 381 SGB 5.

Änderungen an § 2 Absatz 36 BSIG-E

Wortlaut: „„Schadprogramme“ Programme und sonstige informationstechnische Routinen und Verfahren, die dazu dienen, unbefugt Daten zu nutzen oder zu löschen oder unbefugt auf sonstige informationstechnische Abläufe einzuwirken.“

Empfehlung: „„Schadprogramme“ Programme und sonstige informationstechnische Routinen und Verfahren, deren vorrangiger Zweck ist, unbefugt eines oder mehrere Schutzziele von Daten, Diensten oder Systemen, negativ zu beeinträchtigen.“

Begründung: Klarheit der Formulierung und Abgrenzung zum Beispiel von Software, die (auch) für IT-Sicherheitstests, Verschlüsselung von Daten (zum Beispiel Microsoft BitLocker) oder Ähnliches genutzt wird. Gerade die Formulierung „[...] die dazu dienen, unbefugt Daten zu nutzen[...]“ wirkt extrem breit und könnte im Zweifelsfall sogar zum Beispiel Betriebssysteme oder Dokumentenverarbeitungssoftware beinhalten.

Änderungen an § 3 Absatz 1 Satz 17 BSIG-E

Wortlaut: „Einrichtungen der Bundesverwaltung in Fragen der Informationssicherheit, einschließlich der Behandlung von Sicherheitsvorfällen, beraten und unterstützen sowie konkrete, praxisnahe Hilfsmittel zur Umsetzung von Informationssicherheitsvorgaben, insbesondere zur Umsetzung der Vorgaben nach § 30 und § 44, bereitstellen.“

Empfehlung: „Einrichtungen der Bundesverwaltung in Fragen der Informationssicherheit, einschließlich der Behandlung von Sicherheitsvorfällen, beraten und unterstützen sowie konkrete, praxisnahe Hilfsmittel zur Umsetzung von Informationssicherheitsvorgaben, insbesondere zur Umsetzung der Vorgaben nach § 30 und § 44, grundsätzlich öffentlich, bereitstellen.“

Begründung: Soweit es keine schwerwiegenden dagegen sprechenden Gründe gibt, sollten alle praxisnahen Hilfsmittel einem möglichst breiten Empfängerkreis zugänglich gemacht werden, der davon profitieren kann.

Änderungen an § 3 Absatz 1 Satz 18 BSIG-E

Wortlaut: „die Unterstützung darf nur gewährt werden, soweit sie erforderlich ist, um Tätigkeiten zu verhindern oder zu erforschen, die gegen die Sicherheit in der Informationstechnik gerichtet sind oder unter Nutzung der Informationstechnik erfolgen."

Empfehlung: „die Unterstützung darf nur gewährt werden, soweit sie erforderlich ist, um Tätigkeiten zu verhindern oder zu erforschen, die gegen die Sicherheit in der Informationstechnik gerichtet sind."

Begründung: Es könnte ansonsten so ausgelegt werden, dass das Bundesamt Sicherheitsbehörden dabei unterstützen soll Tätigkeiten „zu erforschen", die „unter Nutzung der Informationstechnik erfolgen", was nach hiesigem Erachtens auch Schwachstellenidentifikation zur Ausnutzung beinhalten würde – und damit im Aufgabenbereich der Zentralen Stelle für Informationstechnik im Sicherheitsbereich (ZITiS) liegt. Mangels klar geregeltem Schwachstellenmanagement, sollte auf den Halbsatz verzichtet werden.

Änderungen an § 3 Absatz 1 Satz 20 BSIG-E

Wortlaut: „Einrichtungen der Bundesverwaltung sowie Hersteller, Vertreiber und Anwender in Fragen der Sicherheit in der Informationstechnik, insbesondere unter Berücksichtigung der möglichen Folgen fehlender oder unzureichender Sicherheitsvorkehrungen, beraten, informieren und warnen;"

Empfehlung: „In Fragen der Sicherheit in der Informationstechnik, insbesondere unter Berücksichtigung der möglichen Folgen fehlender oder unzureichender Sicherheitsvorkehrungen, beraten, informieren und warnen;" oder „Hersteller, Vertreiber und Anwender in Fragen der Sicherheit in der Informationstechnik,

insbesondere unter Berücksichtigung der möglichen Folgen fehlender oder unzureichender Sicherheitsvorkehrungen, beraten, informieren und warnen;"

Begründung: Mit Blick auf eine umfassende IT-Sicherheit ist es nicht erklärbar, warum das Bundesamt zwar Hersteller und Betreiber beraten, informieren und warnen können soll, aber nicht zum Beispiel Einrichtungen der Länderverwaltungen, politische Parteien oder den Bundestag. Sollten diese, wie dann auch analog Einrichtungen der Länderverwaltungen, in die Kategorien Hersteller, Vertreiber und Anwender fallen, ist andersherum unklar, warum hier explizit die Einrichtungen der Bundesverwaltungen genannt werden.

Änderungen an § 5 Absatz 1 BSIG-E

Wortlaut: „Zur Wahrnehmung der Aufgaben nach § 3 nimmt das Bundesamt als zentrale Stelle für Meldungen von Dritten Informationen über Sicherheitsrisiken in der Informationstechnik entgegen und wertet diese Informationen aus."

Empfehlung: „Zur Wahrnehmung der Aufgaben nach § 3 nimmt das Bundesamt als zentrale Stelle für Meldungen von Dritten Informationen über Sicherheitsrisiken in der Informationstechnik entgegen und wertet diese Informationen aus. Das Bundesamt wirkt unverzüglich auf die Behebung von Schwachstellen hin. Weisungen die das unterbinden, sind unzulässig."

Begründung: Mangels übergreifendem Schwachstellenmanagement sollten durch klare Formulierungen Rechtssicherheit hergestellt werden und unter anderem dadurch negative Anreize, wie berechtigte Sorgen vor Verwendung der Schwachstelle für staatliche Operationen oder unberechtigter Strafverfolgung, für Sicherheitsforscher:innen abgebaut werden, Schwachstellen an das Bundesamt zu melden.

Änderungen an § 5 Absatz 2 BSIG-E

Wortlaut: „Erfolgt die Meldung nicht anonym, kann der Meldende zum Zeitpunkt der Meldung oder später verlangen, dass seine personenbezogenen Daten nur anonymisiert weitergegeben werden dürfen."

Empfehlung: „Erfolgt die Meldung nicht anonym, kann der Meldende zum Zeitpunkt der Meldung oder später verlangen, dass seine personenbezogenen Daten nur anonymisiert weitergegeben werden dürfen. Weiterhin sollte der Meldende den Bearbeitungsstand seiner Meldung einsehen können."

Begründung: Um positive Anreize zum Melden zu schaffen, sollte es die Möglichkeit für Meldende geben, nachvollziehen zu können, was mit ihren Meldungen passiert ist.

Änderungen an § 7 Absatz 6 BSIG-E

Wortlaut: „Ausgenommen von den Befugnissen nach den Absätzen 1 bis 3 sind Kontrollen der Auslandsinformations- und - kommunikationstechnik nach § 9 Absatz 2 des Gesetzes über den Auswärtigen Dienst, soweit sie im Ausland belegen ist oder für das Ausland oder für Anwender im Ausland betrieben wird."

Empfehlung: Ersatzlos streichen, inklusive aller Verweise.

Begründung: Es ist aus IT-Sicherheitssicht unbegründet, warum es für genau diesen – stark bedrohten – Teil der Informations- und Kommunikationstechnik der Bundesverwaltung eine Ausnahme geben soll. Die Bundesverwaltung sollte sich nicht von IT-Sicherheitsvorgaben ausnehmen, die sie anderen Akteuren auferlegt, ohne auf mindestens vergleichbare Vorgaben für die Bundesverwaltung hinzuweisen, vgl. zum Beispiel § 44 BSIG-E.

Änderungen an § 13 Absatz 1 Satz 1 BSIG-E

Wortlaut: Ergänzung

Empfehlung: „f) Informationen über mehrfache, schwerwiegende Verstöße von Herstellern und Produktverantwortlichen gegen die Leitlinie zum Coordinated Vulnerability Disclosure (CVD)-Prozess bei koordinierten Offenlegungen von Schwachstellen bei denen das Bundesamt als nationaler Koordinator fungiert"

Begründung: Schaffen von weiteren Anreizen für Hersteller/Produktverantwortliche die von Schwachstellen ausgehenden Risiken zeitnah zu mitigieren.

Änderungen an § 14 BSIG-E

Wortlaut: Ergänzung

Empfehlung: „(6) Es ist sicherzustellen, dass nach (1) und (2) erlangte und nach (4) weitergegebene Informationen über Schwachstellen zur Erfüllung der Aufgaben aus § 3 (1) Satz 2 Nr. 1 durch staatliche Stellen, vor allem durch Polizeibehörden von Bund und Ländern, den Verfassungsschutzbehörden von Bund und Ländern, dem Militärischem Abschirmdienst oder dem Bundesnachrichtendienst, nicht zur negativen Beeinträchtigung von einem oder mehrerer Schutzziele verwendet werden."

Begründung: Mangels klar geregeltem Schwachstellenmanagement, muss eine Nutzung so erlangter Informationen für Zwecke abseits der Herstellung der Sicherheit von Informations- und Kommunikationstechnik ausgeschlossen werden. Vor allem da § 3 Absatz 1 Satz 2 Nummer 1 BSIG-E eine intrusive Nutzung durch andere staatliche Stellen nicht umfassend ausschließt.

Änderungen an § 15 Absatz 1 BSIG-E

Wortlaut: „Das Bundesamt kann im Rahmen seiner Aufgaben nach § 3 Absatz 1 Satz 2 Nummer 1, 2, 20 oder 24 zur Detektion von bekannten Schwachstellen und anderen Sicherheitsrisiken bei Einrichtungen des der Bundesverwaltung, bei besonders wichtigen Einrichtungen oder bei wichtigen Einrichtungen Abfragen an den Schnittstellen öffentlich erreichbarer informationstechnischer Systeme zu öffentlichen Telekommunikationsnetzen durchführen, [...]"

Empfehlung: „Das Bundesamt kann im Rahmen seiner Aufgaben nach § 3 Absatz 1 Satz 2 Nummer 1, 2, 20 oder 24 zur Detektion von Schwachstellen und anderen Sicherheitsrisiken bei Einrichtungen der Bundesverwaltung, bei Einrichtungen der Länderverwaltungen, bei besonders wichtigen Einrichtungen oder bei wichtigen Einrichtungen Abfragen an den Schnittstellen öffentlich erreichbarer informationstechnischer Systeme zu öffentlichen Telekommunikationsnetzen durchführen, sofern sofern eine Beeinträchtigung nicht abzusehen ist, [...]"

Begründung: Aus IT-Sicherheit ist ein Ausschluss von Einrichtungen der Länderverwaltungen nicht nachvollziehbar. Weiterhin definiert § 2 Absatz 38 BSIG-E

zwar „Schwachstellen", aber es wird an keiner Stelle definiert, was eine „bekannte Schwachstelle" ist. Daher sollte lediglich der Begriff „Schwachstelle" verwendet werden.

Änderungen an § 16 BSIG-E

Wortlaut: Ergänzung

Empfehlung: „(5) Nach Absatz 1 angeordnete Maßnahmen müssen protokolliert und zur Information von Abgeordneten des Bundestags einsehbar sein. Dabei gilt die Geheimschutzordnung des Deutschen Bundestages."

Begründung: Da es sich hierbei um die Anordnung von teils intrusiven Maßnahmen handelt, ist ein Höchstmaß an Aufsicht geboten.

Änderungen an § 19 BSIG-E

Wortlaut: „Die Bereitstellung von IT-Sicherheitsprodukten durch das Bundesamt nach § 3 Absatz 1 Satz 2 Nummer 15 erfolgt durch Eigenentwicklung oder nach Durchführung von Vergabeverfahren aufgrund einer entsprechenden Bedarfsfeststellung. IT-Sicherheitsprodukte können nur in begründeten Ausnahmefällen durch eine Eigenentwicklung des Bundesamtes zur Verfügung gestellt werden. Die Vorschriften des Vergaberechts und der Bundeshaushaltsordnung bleiben unberührt. Wenn das Bundesamt IT-Sicherheitsprodukte bereitstellt, können die Einrichtungen der Bundesverwaltung oder von ihnen beauftragte Dritte diese Produkte beim Bundesamt abrufen."

Empfehlung: „Die Bereitstellung von IT-Sicherheitsprodukten durch das Bundesamt nach § 3 Absatz 1 Satz 2 Nummer 15 erfolgt durch Eigenentwicklung oder nach Durchführung von Vergabeverfahren aufgrund einer entsprechenden Bedarfsfeststellung. IT-Sicherheitsprodukte können durch eine Eigenentwicklung des Bundesamtes öffentlich zur Verfügung gestellt werden. Die Vorschriften des Vergaberechts. Wenn das Bundesamt IT-Sicherheitsprodukte bereitstellt, können die Einrichtungen der Bundesverwaltung oder von ihnen beauftragte Dritte diese Produkte beim Bundesamt abrufen."

Begründung: Um IT-Sicherheit über alle Sektoren hinweg zu erhöhen, sollten mit Steuermitteln entwickelte IT-Sicherheitsprodukte des Bundesamts öffentlich zugänglich gemacht werden können. Dies sollte möglich sein, ohne dies vorher individuell per Ausnahme von § 63 Absatz 3 BHO regeln zu müssen.

Änderungen an § 29 Absatz 2 BSIG-E

Wortlaut: „Für Einrichtungen der Bundesverwaltung sind die Regelungen für besonders wichtige Einrichtungen anzuwenden, nicht jedoch die Regelungen der §§ 38, 40 Absatz 3 und der §§ 61 und 65. Für Einrichtungen der Bundesverwaltung, ausgenommen das Bundeskanzleramt und die Bundesministerien, sind zusätzlich die Regelungen des § 30 nicht anzuwenden."

Empfehlung: „Für Einrichtungen der Bundesverwaltung sind die Regelungen für besonders wichtige Einrichtungen anzuwenden, nicht jedoch die Regelungen des §§ 38 und 65." oder „Für Einrichtungen der Bundesverwaltung sind die Regelungen für besonders wichtige Einrichtungen anzuwenden, nicht jedoch die Regelungen der §§ 38, 40 Absatz 3 und der §§ 61 und 65. Alle Ressorts erlassen im Einvernehmen mit dem Bundesministerium für Digitales und Staatsmodernisierung [alternativ: CISO-Bund] allgemeine Verwaltungsvorschriften, um die Ziele der NIS-2-Richtlinie ihren Geschäftsbereichen durch ergebnisäquivalente Maßnahmen umzusetzen." oder Änderung an § 44 BSIG-E Absatz 2, siehe untenstehend.

Begründung: Die Bundesverwaltung sollte sich nicht von (Teilen der) IT-Sicherheitsvorgaben ausnehmen, die sie anderen Akteuren auferlegt, ohne auf mindestens vergleichbare Vorgaben für die Bundesverwaltung hinzuweisen.

Änderungen an § 29 Absatz 3 BSIG-E

Wortlaut: „Die Geschäftsbereiche des Auswärtigen Amts und des Bundesministeriums der Verteidigung sowie der Bundesnachrichtendienst und das Bundesamt für Verfassungsschutz sind zusätzlich zu den Regelungen gemäß Absatz 2 von den Regelungen der § 7 Absatz 5 Satz 4, § 10, 13 Absatz 1 Nummer 1 Buchstabe e sowie der §§ 30, 33 und 35 ausgenommen. Das Auswärtige Amt erlässt im Einvernehmen mit dem Bundesministerium für Digitales und Staatsmodernisierung eine allgemeine

Verwaltungsvorschrift, um die Ziele der NIS-2-Richtlinie im Geschäftsbereich des Auswärtigen Amtes durch ergebnisäquivalente Maßnahmen umzusetzen."

Empfehlung: Ersatzlos streichen, inklusive aller Verweise, oder „Die Geschäftsbereiche des Auswärtigen Amts und des Bundesministeriums der Verteidigung sowie der Bundesnachrichtendienst sind zusätzlich zu den Regelungen gemäß Absatz 2 von den Regelungen der § 7 Absatz 5 Satz 4, § 10, 13 Absatz 1 Nummer 1 Buchstabe e sowie der §§ 30, 33 und 35 ausgenommen. Das Auswärtige Amt, das Bundesministerium der Verteidigung und das Bundeskanzleramt erlassen im Einvernehmen mit dem Bundesministerium für Digitales und Staatsmodernisierung [alternativ: CISO-Bund] allgemeine Verwaltungsvorschriften, um die Ziele der NIS-2-Richtlinie ihren Geschäftsbereichen durch ergebnisäquivalente Maßnahmen umzusetzen."

Begründung: Die Bundesverwaltung sollte sich nicht von (Teilen der) IT-Sicherheitsvorgaben ausnehmen, die sie anderen Akteuren auferlegt, ohne auf mindestens vergleichbare Vorgaben für die Bundesverwaltung hinzuweisen.

Änderungen an § 38 Absatz 3 BSIG-E

Wortlaut: „Die Geschäftsleitungen besonders wichtiger Einrichtungen und wichtiger Einrichtungen müssen regelmäßig an Schulungen teilnehmen, um ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken und von Risikomanagementpraktiken im Bereich der Sicherheit in der Informationstechnik zu erlangen sowie um die Auswirkungen von Risiken sowie Risikomanagementpraktiken auf die von der Einrichtung erbrachten Dienste beurteilen zu können."

Empfehlung: „Die Geschäftsleitungen besonders wichtiger Einrichtungen und wichtiger Einrichtungen müssen regelmäßig erfolgreich an geeigneten Schulungen mit standardisierten Lernerfolgsprüfungen teilnehmen, um ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken und von Risikomanagementpraktiken im Bereich der Sicherheit in der Informationstechnik zu erlangen sowie um die Auswirkungen von Risiken sowie Risikomanagementpraktiken auf die von der Einrichtung erbrachten Dienste beurteilen zu können." oder „Die Geschäftsleitungen besonders wichtiger Einrichtungen und wichtiger Einrichtungen müssen regelmäßig erfolgreich an geeigneten Schulungen mit standardisierten

Lernerfolgsprüfungen teilnehmen, um ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken und von Risikomanagementpraktiken im Bereich der Sicherheit in der Informationstechnik zu erlangen sowie um die Auswirkungen von Risiken sowie Risikomanagementpraktiken auf die von der Einrichtung erbrachten Dienste beurteilen zu können. Das Bundesamt stellt hierzu öffentlich einen Musterlehrplan bereit, den Prüfungsanbieter aufgreifen sollten." oder ersatzlos streichen, inklusive aller Verweise.

Begründung: Eine reine Teilnahme an Schulungen ohne nachgewiesenen Qualitätsstandard und Erfolgsprüfung ist ineffektiv und ineffizient. Weiterhin ist unklar, wie die hohe Anzahl an notwendigen Schulungen unter Wahrung von Lernerfolgen durchgeführt werden kann.

Änderungen an § 43 Absatz 2 BSIG-E

Wortlaut: „Die Leitung der Einrichtung der Bundesverwaltung muss regelmäßig an Schulungen teilnehmen, um ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken und von Risikomanagementpraktiken im Bereich der Informationssicherheit zu erlangen sowie die Auswirkungen von Risiken sowie Risikomanagementpraktiken auf die von der Einrichtung erbrachten Dienste beurteilen zu können."

Empfehlung: „Die Leitung der Einrichtung der Bundesverwaltung muss regelmäßig an vom Bundesamt akkreditierten oder durch das Bundesamt durchgeführten Schulungen mit standardisierten Lernerfolgsprüfungen teilnehmen, um ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken und von Risikomanagementpraktiken im Bereich der Informationssicherheit zu erlangen sowie die Auswirkungen von Risiken sowie Risikomanagementpraktiken auf die von der Einrichtung erbrachten Dienste beurteilen zu können." oder ersatzlos streichen, inklusive aller Verweise.

Begründung: Eine reine Teilnahme an Schulungen ohne nachgewiesenen Qualitätsstandard und Erfolgsprüfung ist ineffektiv und ineffizient.

Änderungen an § 43 Absatz 5 BSIG-E

Wortlaut: „Ausgenommen von der Pflicht nach Absatz 5 Satz 3 sind der Bundesnachrichtendienst und das Bundesamt für Verfassungsschutz."

Empfehlung: Ersatzlos streichen, inklusive aller Verweise.

Begründung: Mangels eines klar geregelten Schwachstellenmanagements sollten dem Bundesamt alle Informationen zur Verfügung gestellt werden, die es für die Erfüllung seiner Aufgaben benötigt.

Änderungen an § 44 Absatz 2 BSIG-E

Wortlaut: „Das Bundeskanzleramt und die Bundesministerien müssen als zusätzliche Mindestanforderungen die BSI-Standards und das IT-Grundschutz-Kompendium des Bundesamtes (IT-Grundschutz) in den jeweils geltenden Fassungen einhalten."

Empfehlung: „Die Einrichtungen der Bundesverwaltung müssen als zusätzliche Mindestanforderungen die BSI-Standards und das IT-Grundschutz-Kompendium des Bundesamtes (IT-Grundschutz) in den jeweils geltenden Fassungen einhalten."

Begründung: Aus IT-Sicherheitssicht nicht nachvollziehbar, dass alle Einrichtungen der Bundesverwaltung außer Kanzleramt und Bundesministerium diese IT-Sicherheitsanforderungen nicht erfüllen müssen.

Änderungen an § 48 BSIG-E

Wortlaut: „Die Bundesregierung bestellt eine Koordinatorin oder einen Koordinator für Informationssicherheit."

Empfehlung: Eine Ausgestaltung der Befugnisse und Ressourcen dieser Stelle ist notwendig, bevor dieser Paragraph so verabschiedet werden kann. Für Details, siehe Empfehlungen zu *Koordinator:in für Informationssicherheit*.

Begründung: Während die Idee gut und eine Umsetzung der Anforderungen aus der NIS-2-Richtlinie ist, hat man sich hier offenbar keine abschließenden Gedanken über (wichtige) Details gemacht.

Änderungen an § 55 BSIG-E

Wortlaut: Freiwilliges IT-Sicherheitskennzeichen

Empfehlung: Es wird zeitnah eine unabhängige Prüfung des konkreten Beitrags vom „Freiwilligen IT-Sicherheitskennzeichen" für die IT-Sicherheit in Deutschland empfohlen. Sollte es sich als nicht geeignet erweisen, wird ein ersatzloses Streichen des §, inklusive aller Verweise und Verordnungen.

Begründung: Es ist unklar, ob das Freiwillige IT-Sicherheitskennzeichen einen Mehrwert für die IT-Sicherheit in Deutschland liefert. Speziell mit Blick auf die zur Implementierung beim Bundesamt notwendigen Ressourcen, sowie die ohnehin zukünftig umzusetzenden Vorgaben für Hersteller und Produktverantwortliche, die sich aus dem Cyber Resilience Act (CRA) für sie ergeben.

Änderungen an § 56 Absatz 4 BSIG-E

Wortlaut: „Das Bundesministerium des Innern bestimmt durch Rechtsverordnung, die nicht der Zustimmung des Bundesrates bedarf, [...]"

Empfehlung: „Das Bundesministerium des Innern bestimmt durch Rechtsverordnung, die der Zustimmung von Bundestag und Bundesrat bedarf, [...]"

Begründung: Änderungen an dieser Rechtsverordnung können für Privatwirtschaft und Gesellschaft in Deutschland weitreichende Folgen im Bereich IT-Sicherheit und anderer Bereiche haben. Daher sollte geprüft werden, ob eine Einvernehmensregelung der Exekutive der Schwere der Veränderungen hier wirklich Rechnung trägt oder die Legislative zusätzlich eine Rolle spielen müsste.

3. Danksagung

Der Sachverständige bedankt sich bei den Vertreter:innen aus Verwaltung, Wirtschaft, Wissenschaft und Zivilgesellschaft für den Informationsaustausch, der maßgeblich als Basis für diese Stellungnahme diente.