Andreas Könen

Brandenburgisches Institut für Gesellschaft und Sicherheit (BIGS) gGmbH

Dianastraße 46

14482 Potsdam

Deutscher Bundestag

Ausschuss für Inneres und Heimat

Ausschussdrucksache
20(4)523 F

Schriftliche Stellungnahme im Rahmen der Sachverständigenanhörung zum NIS2-Umsetzungs- und Cybersicherheitsstärkungsgesetz

Allgemeine Vorbemerkung zur Person

- Dipl.-Mathematiker, Thematischer Schwerpunkt algebraische Zahlentheorie u.a. mit Bezügen zur Public-Key-Kryptographie.
- Tätigkeiten im BND, BSI und BMI, zuletzt bis 31.03.2024 als Abteilungsleiter Cyber- und Informationssicherheit im Bundesministerium des Innern und für Heimat
- Aktuell im einstweiligen Ruhestand, ehrenamtliche Tätigkeit als Senior Fellow des Brandenburgischen Instituts für Gesellschaft und Sicherheit
- Mit dem NIS2UmsuCG war ich auch dienstlich im BMI befasst, hier vertrete ich meine persönliche fachliche, wissenschaftliche und politische Position zum vorliegenden Entwurf. Dabei stehe ich zu meiner Verantwortung für einen großen Teil der Implementierung der NIS2-Richtlinie in der aktuellen Fassung.

Grundsätzlicher Ansatz der Cybersicherheitsregulierung EU und national

- Grundsätzliche Aspekte zur NIS2-Richtlinie der EU
    - Angesichts der sich stetig verstärkenden Cyberbedrohungslage in den und gegen die Mitgliedstaaten der Europäischen Union wurde deutlich, dass zum Schutz von Unternehmen und zur Sicherstellung der Versorgung von Bürgerinnen und Bürgern der EU eine über die NIS-Richtlinie hinausgehende Regulierung von Unternehmen in den Sektoren der Kritischen Infrastrukturen erforderlich war.
    - Dabei zeigten die Erfahrungen mit dem IT-SiG 1.0, der NIS1-Richtlinie und dem IT-SiG 2.0 deutlich, dass Regulierung zu einer echten Erhöhung des Cybersicherheitsniveaus führt. Im Austausch des BSI und des BMI mit den deutschen Unternehmen und Wirtschaftsverbänden wurde immer wieder zum Ausdruck gebracht, dass die genannten Gesetze einen tatsächlichen und nachweisbaren Effekt zu einer verbesserten Aufstellung der deutschen Wirtschaft in der Cybersicherheit hatten.
    - Gerade aber im Bereich der nicht-regulierten Unternehmen, aber auch in der öffentlichen Verwaltung, speziell den Kommunen und Kreisen, führte die erhöhte Cyberbedrohungslage zu einer Vielzahl von Cybersicherheitsvorfällen. Hier bestand und besteht Handlungsdruck.
    - Dabei ist es von herausragender Bedeutung, dass eine weitergehende europäische Regulierung sowohl in der horizontalen (d.h. über die verschiedenen Sektoren der Kritischen Infrastrukturen hinweg) als auch in der Vertikalen (von großen zu kleinen Unternehmen, von der Verwaltung der EU und des Bundes bis auf die kommunale Ebene)

harmonisierte Cybersicherheitsanforderungen stellt. Entscheidend ist aber auch die ebenen-adäquate Umsetzbarkeit.

- Konsequenterweise erweitert die EU-KOM mit dem Entwurf der NIS2-Richtlinie daher den Umfang regulierter Unternehmen deutlich, führt aber den grundsätzlich auf Versorgungskritikalität beruhenden Ansatz aus der NIS1-Richtlinie (wie auch im IT-SiG 1.0 und IT-SiG 2.0) nicht fort!
- Die EU-Kommission wählt einen Sektor-orientierten Ansatz mit pauschalen Schwellenwerten bei Mitarbeitendenzahlen und Umsatz der Unternehmen.
- Dies bedeutet insbesondere für Deutschland eine grundsätzliche Änderung des methodischen Vorgehens im Vergleich zu IT-SiG 1.0, NIS-1 und IT-SiG 2.0.
- Als Begründung führte die EU-KOM die Feststellung ins Feld, dass es auf diesem Weg für Unternehmen und Behörden leichter werde, die eigene Betroffenheit durch die Regulierung festzustellen. Dies sei notwendig, da viele Mitgliedstaaten der EU die NIS1-Richlinie vor allem auch wegen der komplexen Kritikalitätsregeln nicht umgesetzt hätten.
- Aber: Die gewählten Schwellenwerte und die weitere Methodik der Regulierung (s.u.) führen zu einer drastisch erhöhten Zahl regulierter Unternehmen (gut), zu einer Abgrenzungsproblematik für Unternehmen im Schwellenbereich (schlecht), zu einer teilweise vagen Differenzierung zwischen "essential" und "important" Einrichtungen (schwierig) sowie zu einer Verdrängung des Begriffes "Kritische Infrastruktur resp. Einrichtung" (schlecht).
- Die eigene Betroffenheit durch die Regulierung ist gerade für viele Unternehmen im Grenzbereich der Schwellenwerte schwer durchschaubar, die pauschale Regelung nach Personalstärke und Umsatz statt nach Kritikalität erscheint nicht sachgerecht, aber leider auch bei einer erheblichen Anzahl von Unternehmen auch nicht leichter umsetzbar.
- Die Öffentliche Verwaltung wird durch die NIS2-Richlinie allerdings nicht in der gleichen Weise wie die Wirtschaft reguliert:
- Für den Bund und die Bundesländer wird durch NIS2 jeweils nur die oberste, sprich Ministerialebene reguliert, eine Problematik, die sich im NIS2UmsuCG leider ausgewirkt hat (siehe unten).
- Grundsätzlich ist keine Regulierung der Kommunalverwaltung sowie der nachgeordneten Behörden in Bund und Ländern vorgesehen.
- Die Regulierung der Öffentlichen Verwaltung auf Ebene der Bundesländer ist aufgrund unserer föderalen Ordnung durch diese selbst vorzunehmen, daher konnte das NIS2UmsuCG als nicht im Bundesrat zustimmungspflichtiges Gesetz vorgelegt werden.

- Grundsätzliche Aspekte zur nationalen Implementierung der NIS2-Richtlinie
  - Im Lichte der vorgenannten Änderungen in der NIS2-Richtlinie steht die Umsetzung des neuen Regulierungsmaßstabes klarerweise im Mittelpunkt.
  - Hierbei gilt es, bewährte Methoden und Strukturen aus dem bisher geltenden Cybersicherheitsgesetz zu übertragen. Dies kommt besonders durch die Beibehaltung des Begriffs des Betreibers kritischer Anlagen in Artikel 1, §31zum Tragen und ist positiv zu bewerten.
  - Auch die neue Struktur des BSIG (Artikel 1) ist hilfreich, vor allem die vorangestellten Begriffsbestimmungen in Artikel 1, §2.

- Durch die zeitgleich erforderliche Implementierung der europäischen CER-Richtlinie als KRITIS-Dachgesetz in nationales Recht ergibt sich die Chance, beide Rechtssetzungen aufeinander abzustimmen und damit harmonisierte Begriffe und Vorschriften zu implementieren.
- Vor allem ist aber damit zugunsten der regulierten Wirtschaft und der Bundesverwaltung die Einrichtung eines „single point of contact“ bei BBK und BSI möglich.
- Insbesondere ist im NIS2UmsuCG eine deutliche Stärkung der Rolle des BSI als nationaler Cybersicherheitsbehörde möglich und erforderlich.

Bewertung des NIS2UmsuCG im Einzelnen

Artikel 1 BSI-Gesetz

- §1 wird gegenüber dem gültigen BSI-G unverändert übernommen. Damit wird die Rolle des BSI in der Cybersicherheitsarchitektur Deutschlands unverändert beibehalten, Anpassungen zur diskutierten unabhängigeren Aufstellung des BSI wurden bisher nicht vorgenommen. Eine deutlichere Betonung der wissenschaftlich-fachlichen Unabhängigkeit des BSI könnte hier durchaus zur sichtbar neutralen Rezeption des BSI beitragen.
  Eine „Unabhängigkeit“ des BSI von etwa einer Fach- oder gar Rechts- oder Dienstaufsicht erscheint aber gerade angesichts der neuen hoheitlichen Aufgaben des BSI im Rahmen von NIS2 (siehe unten zu weiteren Regelungen dort) im Sinne einer Kontrolle der Exekutive nicht angebracht.
- §2: Wie bereits angemerkt, ist die Einführung von Begriffsbestimmungen in §2 positiv zu werten, die gewählten Formulierungen werden in einzelnen Fällen in Kommentaren kritisch bewertet. Aus Sicht des Gutachters besteht hier vor allem berechtigte Kritik an der gewählten Definition der „Forschungseinrichtung“, die allerdings aus der NIS2-Richtlinie übernommen wurde:
  - Der Sektor Forschung wird gemäß der Begriffsdefinition „Forschungseinrichtung“ auf angewandte Forschung mit kommerziellem Zweck begrenzt. Hier sollten alle öffentlich finanzierten Forschungseinrichtungen einbezogen werden.
- §7(4), 4.: Der Koordinator für Informationssicherheit des Bundes wurde gegenüber der dritten Version gestrichen und sollte wieder eingefügt werden.
- §15(1): Die Erweiterung der Befugnisse des BSI, „Schwachstellen-Scans“ vorzunehmen, ist in §15(1) erweitert worden. Dies wird begrüßt, ebenso die Vereinfachung der dabei angewandten Vorgehensweise. Leider bleibt die Erweiterung hinter den Erwartungen zurück, wünschenswert wäre eine Erweiterung der Befugnisse des BSI auf den gesamten nationalen Ausschnitt des Internets.
- §28: Der Anwendungsbereich des NIS2UmsuCG entspricht der Vorgabe der NIS2-Richtlinie und geht in positiver Weise hinsichtlich des Differenzierungsmerkmals „Betreiber kritischer Anlagen“ darüber hinaus. ZU beachten bleibt, dass erst mit der Aktualisierung der Verordnung gemäß §56(4) (KRITIS-VO) in Verbindung mit der Bestimmung der Einrichtungsarten gemäß Anlage 1 letztendlich Rechtssicherheit bezüglich des Anwendungsbereiches geschaffen wird.
  Darüber hinaus bleibt festzuhalten, dass IT-Dienstleister, die Dienste ausschließlich für Landes- und Kommunalverwaltungen erbringen, vom Anwendungsbereich nicht erfasst werden. Dies ist angesichts der Cybersicherheitsvorfälle gerade bei diesen Unternehmen nicht verständlich und sollte spätestens in den Umsetzungsgesetzen der Bundesländer Berücksichtigung finden.
- §29(1): Hier sind erste Folgen der uneinheitlichen Regelungen der NIS2-Richtlinie bei der nationalstaatlichen Umsetzung erkennbar: Eine reine Regulierung der Öffentlichen Verwaltung

auf Bundesebene, dazu Ausnahmen für die Bundesbank und die Institutionen der Sozialen Sicherung. Gerade bei letzteren Einrichtungen ist nicht verständlich, warum hier etwa ein geringerer Schutzbedarf bestehen könnte. Damit wird ein harmonisierter Schutz und insbesondere auch eine gemeinsame Cybersicherheitslage mit diesen Einrichtungen erschwert oder sogar verhindert.

- §29(2): Mit den Regelungen dieses Absatzes bedeuten einen deutlichen Rückschritt für die Cybersicherheit der Bundesverwaltung. Insbesondere die Unterscheidung des Satzes 2 zur Anwendbarkeit des §30 für die Ministerien einschließlich des Kanzleramtes im Gegensatz zu den übrigen Bundesbehörden führt zu einer 2-Klassen-Einteilung beim Schutzniveau in der Bundesverwaltung und widerspricht damit ausdrücklich dem Harmonisierungsziel der NIS2-Richtlinie (vergleiche hierzu auch §44). §30 regelt das harmonisierte Risikomanagement aller besonders wichtigen und wichtigen Einrichtungen und damit die robuste Aufstellung gegenüber allen Cybersicherheitsrisiken.
  Ebenso sind auch die Ausnahmen des ersten Satzes von zumindest Teilen des §40(3) (gemeinsame Auswertung und Bewertung der Cybersicherheitslage) und vom §61nicht nachvollziehbar. Letzterer Paragraph sollte mindestens in einer für die Bundesbehörden angepassten Form und in Verbindung mit den Aufgaben eines Koordinators für die Informationssicherheit des Bundes auch für die Bundesverwaltung Gültigkeit erlangen.

- §29(3): Die bisherigen Ausnahmen für das Auswärtige Amt und das BMVg, so wie sie auch bereits in den bestehenden §7(5) und (6) des IT-SiG 2.0 abgebildet sind (jetzt §7(6) und §7(7)), sind absolut ausreichend, um den spezifischen Anforderungen dieser beiden Ressorts und ihrer IT-Infrastrukturen gerecht zu werden und haben sich vor allem im Falle des BMVg bewährt. Die Ausnahmen für den Bundesnachrichtendienst und das Bundesamt für Verfassungsschutz sind dort nachvollziehbar, wo es um den Schutz der nachrichtendienstlichen Informationen und Prozesse geht und hätten über das Sicherheitsüberprüfungsgesetz in Verbindung mit der Verschlusssachenanweisung abgebildet werden können.
  In keinem Falle sind aber wie bei §29(2) Ausnahmen von den Regelungen des §30 gerechtfertigt (siehe oben).

- §30: Der risiko-orientierter Ansatz für das Informationssicherheitsmanagement der besonders wichtigen und wichtigen Einrichtungen ist richtig, wichtig und gut. Er bildet den Kern des Regelungsansatzes der NIS2-Richtlinie und sollte daher ausnahmslos für den gesamten Anwendungsbereich der NIS2-Richtlinie Gültigkeit besitzen.
  Im Einzelnen sind dabei noch positiv die Regelungen des §30(6), (8) und (9) zu nennen, die einerseits die Grundlage für die Verwendung zertifizierter IKT-Produkte, IKT-Dienste und IKT-Prozesse gemäß dem Cyber Security Act (CSA) sowie dem Cyber Resilience Act (CRA) der EU bilden und andererseits die Nutzung branchenspezifischer Sicherheitsstandards befördern.
  Kritikwürdig ist dagegen die Aufzählung konkreter Maßnahmen in §30(2). Diese ist künstlich, entscheidend ist konzeptioneller Ansatz beim Risikomanagement wie etwa im IT-Grundschutz und den BSI-Standards niedergelegt.

- §31: Wie bereits dargelegt sind die besonderen Regelungen des §31 für die Betreiber kritischer Anlagen konsequent in der Fortführung des Regelungsansatzes des IT-SiG 1.0 und 2.0 und in der Harmonisierung zu den Regelungen des KRITIS-DG. Die Wichtigkeit dieser Einrichtungen für die Resilienz der nationalen Volkswirtschaft wird damit auch angesichts der seit 2022 verstärkten Bedrohungen durch Cybersabotage hervorgehoben und zusätzliche Maßnahmen von den Betreibern abverlangt. Aus meiner Sicht fehlt hier lediglich ein Bezug zu den Regelungen gemäß §56(4) (KRITIS-VO).

- §32: Mit der Meldepflicht wird neben dem Risikomanagement die zweite Säule der harmonisierten Cybersicherheitsanforderungen aufgebaut. Die Cybersicherheitslage Deutschland und in der europäischen Union erfordert eine solche Meldepflicht, die kurzen Fristen

halte ich gerade angesichts der Notwendigkeit von schnellen Cyberabwehrmaßnahmen für angemessen und erforderlich zum Schutz potentiell weiterer Betroffener.
Allerdings fehlen hier Anforderungen an die Wirtschaft, Sektoren und Branchen, sich gegenüber dem Staat (Bund, Länder und Kommunen) auch selbst hinsichtlich der Cybersicherheitslage organisatorisch aufzustellen und mit brachen- oder sektorspezifischen CERT's, CSIRT's oder SOC's den Behörden als Ansprechpartner gegenüber zu treten.

- §32(6): Das in §32(6) formulierte Unterstützungsangebot des BSI bleibt als Kann-Vorschrift weit hinter den Zielsetzungen der NIS2-Richtlinie zurück. In Abstimmung mit den auf EU-Ebene durch ENISA zu koordinierenden Unterstützungsmaßnahmen durch alle Mitgliedstaaten der EU ist eine Soll-Vorschrift wäre hier das Mindestmaß. Weiterhin bietet dieser Absatz die Möglichkeit, einen rechtlichen Anker für die Etablierung gemeinsamer Strukturen mit der Wirtschaft zur Unterstützung Betroffener bei (erheblichen) Sicherheitsvorfällen zu schaffen (es muss ja nicht unbedingt das Cybersicherheitsnetzwerk oder das Cyberhilfswerk sein).

- §36: Die hier normierten Informationspflichten für das BSI sind richtig und wichtig, aber auch mit Blick auf die Anmerkungen zu §32(6) sollte die Informationsübermittlung insbesondere bei Unterstützungsleistungen des BSI erweitert werden und korrespondierend zu §32 hier auch verankert werden.
  Dabei bildet ein Information Sharing Portal beim BSI eine wesentliche technische Komponente und ist Teil der dringend erforderlichen Digitalisierung der Informationssicherheit.

- §38: Die Anforderungen an Geschäftsleitungen halte ich trotz der vielfältigen verständlichen Stellungnahmen aus der Wirtschaft für richtig. In meiner beruflichen Laufbahn sind mir in allen Bereichen von Wirtschaft und Verwaltung immer wieder und damit zu oft Personen (allerdings handelt es sich um „schwarze Schafe" im Vergleich zur großen Zahl versierter Menschen) begegnet, die gegenüber den Risiken der Digitalisierung und des Cyberraums völlig ignorant waren.

- §39: Zu diesen Regelungen steht ebenfalls die Harmonisierung mit dem KRITIS-DG aus.

- §40: Auch §40 harrt der Harmonisierung mit dem KRITIS-DG. Hier ist eine entsprechende Normierung der Rolle des BBK erforderlich. Eine verbesserte Einbindung der Bundesländer sollte durch eine Zentralstellenfunktion des BSI befördert werden. Erneut ist auch der Hinweis angebracht, dass eine Aufstellung der Wirtschaft z.B. mit Branchen- oder Sektor-CERTs notwendig ist und normiert werden sollte.

- §41 entspricht bisherigem §9b BSIG, die Übernahme in die neue Gesetzgebung ist richtig und angesichts sowohl der wirtschaftspolitischen als auch weltpolitischen Lage sehr wichtig.
  Allerdings hat §41 alias BSIG §9b erheblichen Verbesserungsbedarf:

    - Eine Erweiterung der des Anwendungsbereichs des §41 über die bisher regulierte Telekommunikations- und Energiebranche hinaus ist dringend erforderlich. Hier seien beispielhaft etwa die hochrelevanten Sektoren Gesundheit und Verkehr genannt.

    - Das hinter §41 liegenden Verwaltungsverfahren muss schon aufgrund der im Telekommunikationssektor gemachten Erfahrungen angepasst werden. Das Verfahren muss etwa dem zukünftig um ein Vielfaches höheren Fallzahlen standhalten, Entsprechendes gilt hinsichtlich der steigenden juristischen und fachlichen Anforderungen.

    - Grundsätzlich sollte das Verfahren von einer Genehmigungsfiktion nach Fristablauf auf einen Genehmigungsvorbehalt umgestellt werden.

    - Nicht-digitale technische Produkte und Anlagen, die Einsatz in kritischen Anlagen finden, unterliegen ähnlichen Risiken wie digitale Produkte. Daher sollten auch hier

entsprechende gesetzliche Regelungen zur Vertrauenswürdigkeit von Herstellern eingeführt werden.

- Daher empfehle ich eine zentrale Regelung für die analoge und die reale Welt im KRITIS-DG und damit eine Überführung des §41 NIS2UmsuCG in das KRITIS-DG!

- §44 (1) und (2): Durch die Regelungen dieser beiden Absätze werden die aktuell aufgrund eines Kabinettbeschlusses geltenden Regelungen des Umsetzungsplanes Bund 2.0 für alle Bundeseinrichtungen mit Ausnahme des Kanzleramtes und der Bundesministerien abgesenkt. Die NIS-2-Richtlinie eröffnet diese Möglichkeit in Art. 5. Offenbar macht die Bundesregierung aufgrund von Ressortwiderständen von dieser Möglichkeit keinen Gebrauch.
  Damit werden zum ersten Mal in Deutschland existierende Cybersicherheitsanforderungen gestrichen und in diesem Falle die Anforderungen gemäß IT-Grundschutz gegenüber allen Bundesbehörden mit Ausnahme des Kanzleramtes und der Bundesministerien fallen gelassen. Insbesondere muss auch das BSI seine eigenen Anforderungen gemäß IT-Grundschutz nicht mehr erfüllen. Zur Bewertung und zu Schlussfolgerungen hieraus siehe unten.
  Darüber hinaus ist in §44(2) die Nennung des IT-Grundschutzkompendiums sachfremd. Sachlich entscheidend ist die Einhaltung der Anforderungen des IT-Grundschutzes und der entsprechenden BSI-Standards. Die Form der Anforderungen als Kompendium ist irrelevant und wird sich im Rahmen der Digitalisierung der Informationssicherheit hochwahrscheinlich ändern. Auch die weiteren den IT-Grundschutz betreffenden Formulierungen in §44(2) „Der IT-Grundschutz wird durch das Bundesamt … bis zum 1. Januar 2026 modernisieren und fortentwickeln." sind mit Blick auf den IT-Grundschutz als Standard und Methodik der Informationssicherheit ebenfalls sachfremd, fehlerhaft, wissenschaftlich nicht haltbar, in sich widersprüchlich und ohnehin kein Gegenstand gesetzlicher Regelungen. Zur Bewertung und Empfehlungen hierzu siehe unten.

- Die Regelungen der §§ 45, 46 und 47 zur gesetzlichen Verankerung der Informationssicherheitsbeauftragten sind absolut begrüßenswert und sichern die Rolle der „ITSiBe's" nun endlich gesetzlich ab. Dennoch wäre auch hier Raum für weitere Verbesserungen, z.B. die Anbindung an den Koordinator für Informationssicherheit des Bundes.

- §48: Die Einrichtung des/der Koordinator/-in für Informationssicherheit des Bundes ist ebenfalls absolut begrüßenswert. Allerdings ist aufgrund des Wegfalls der §§ 49 und 50 des dritten Entwurfs des NIS2UmsuCG die Rolle des Koordinators nun völlig inhaltslos. Als Minimalanforderung sollten daher diese §§ wieder Eingang in das Gesetz finden (siehe Anlage). Weitere Bewertungen und Anforderungen siehe unten.

- Die in §56 normierten Rechtsverordnungen gemäß den Absätzen (3) (Zertifikate), (4) (KRITIS-VO) und (5) (Sicherheitsvorfälle) sind für die untergesetzliche Umsetzung der NIS-2-Richtlinie wesentlich. Allerdings sollte in §56(5) einheitlich nur das Benehmen mit den Ressorts vorgesehen werden.

- §61: Die Bundesverwaltung sollte im Ganzen nicht von der Anwendung dieses Paragraphen ausgenommen werden, siehe auch Kommentar zu §29.

- §64: Die hier getroffenen besonderen Regelungen für Institutionen der sozialen Sicherung sind im Sinne der unter §29 getroffenen Ausnahmeregelungen konsistent, widersprechen aber einer harmonisierten Aufstellung angesichts der auf alle Einrichtungen wirkenden gleichen Bedrohungslage. Daher erneuter Vorschlag der Streichung der Sonderrolle der Institutionen der sozialen Sicherung.

Artikel 17 Änderung des Energiewirtschaftsgesetzes

- Die hier vorgesehenen Änderungen sind im Wesentlichen deckungsgleich mit den Regelungen im Artikel 1 und schreiben eine besondere Rolle der Bundesnetzagentur in der Cybersicherheit fest.

Ohne hierauf im Einzelnen einzugehen, erscheinen die getroffenen Sonderregelungen unnötig. Für die Energiewirtschaft entsteht dadurch eine komplexere Regelungslandschaft als für andere Sektoren.

Artikel 26 Änderung des Telekommunikationsgesetzes

- Die hier vorgesehenen Änderungen sind im Wesentlichen deckungsgleich mit den Regelungen im Artikel 1 und schreiben eine besondere Rolle der Bundesnetzagentur in der Cybersicherheit fest. Ohne hierauf im Einzelnen einzugehen, erscheinen die getroffenen Sonderregelungen unnötig. Für die Telekommunikationswirtschaft entsteht dadurch eine komplexere Regelungslandschaft als für andere Sektoren.

Weitere Anmerkungen zur Umsetzung der EU-Fassung der NIS2-Richtlinie

- Mit dem NIS2UmsuCG wird der Anteil der NIS2-Richtlinie umgesetzt, der nationale Rechtssetzung gegenüber der Wirtschaft und der öffentlichen Verwaltung erfordert und in der alleinigen Rechtssetzungskompetenz des Bundes liegt.
- Damit kommt den Bundesländern die Aufgabe zu, nun für eine Umsetzung der NIS2-Richtlinie auf Landesebene zu sorgen. Dem sind einige Bundesländer bereits nachgekommen, wobei neben einer Umsetzung als Landesgesetz auch Verordnungen oder Erlasse/Weisungen möglich sind. Entscheidend ist allerdings, dass sich die Länder in die Lage versetzen, den Meldeverpflichtungen gegenüber dem Bund nachzukommen und von dort auch Meldungen entgegen nehmen zu dürfen(!).
- In der Umsetzung der NIS2-Richtlinie bleiben dem nationalen Gesetzgeber auch einige Freiheiten, die z.B. die Umsetzung von Empfehlungen aus der NIS2-Richtlinie in den nationalen Gesetzestext betreffen. So wurde etwa Art. 24, Abs. 1, Satz 2 nicht übertragen, der eine Empfehlung an die Mitgliedstaaten zur Förderung qualifizierter Vertrauensdienste angeht. Hier sind auch andere (politische) Mechanismen als Maßnahme vorstellbar.
- Große Teile der NIS2-Richtlinie betreffen die institutionelle Implementierung der NIS2-Richtlinie auf EU-Ebene und in der Kommunikation mit den Mitgliedstaaten. Diese Anforderungen bedürfen keiner expliziten Umsetzung im NIS2UmsuGC sondern gelten unmittelbar, dies betrifft etwa
    - Die in den Artikeln 7 bis 13 genannten Aufgaben zur Nationalen Cybersicherheitsstrategie, den zuständigen Behörden (in Deutschland gemäß BSIG-E dem BSI), dem nationalen Rahmen für das Cyberkrisenmanagement etc.
    - Die in Artikel 14-17 genannten Institutionen auf EU-Ebene wie der Kooperationsgruppe, dem CSIRT-Netzwerk und EU-Cyclone.
- Diese Aufgaben sowie die Vertretung in den genannten Strukturen fällt dabei auf nationaler Ebene dem BSI und dem BMI zu. Auch hierfür ist entsprechende Haushaltsvorsorge zu betreiben.

Anmerkungen zu den Querverbindungen mit der KRITIS-DG

- Bezüge zum KRITIS-DG ergeben sich vor allem in den Paragraphen
    - §31 Besondere Anforderungen an das Risikomanagement von Betreibern kritischer Anlagen
    - §39 Nachweispflichten für Betreiber kritischer Anlagen
    - §40 Nationale Verbindungsstelle
    - §41 Untersagung des Einsatzes kritischer Komponenten
- Hier ist eine Harmonisierung der Vorschriften und Anforderungen sowie eine Synchronität der Vorgehensweise zwischen den Anwendungsbereichen von NIS2 und CER resp. NIS2UMsuCG und KRITIS-DG erforderlich.

- Insoweit ist der fehlende Kabinettbeschluss zum KRITIS-DG ein echter Hemmschuh für die weiteren parlamentarischen Prozess bei NIS2.
- In praktischer Hinsicht möchte ich noch einmal folgende zwei Anforderungen benennen, deren Umsetzung gerade für die Wirtschaft (aber auch die Verwaltung!) zur Minimierung von Aufwänden essentiell sind:
    - Etablierung eines(!) „Single-Point-of-Contact“ bei BBK und BSI in dem Sinne, dass für die Wirtschaft die Adressierung einer der beiden Behörden ausreicht, alles Weitere wird im zwischenbehördlichen Verfahren geklärt,
    - Verschiebung in das KRITIS-DG und Novellierung des §41 BSIG-E alias „§9b“.

Fazit

Gesamtbewertung

- Das NIS2UmsuCG befindet sich zum richtigen Zeitpunkt (wenn auch verspätet) im parlamentarischen Verfahren:
    - Der durch den russischen Angriffskrieg gegen die Ukraine deutlich verschärften Cybersicherheitslage muss durch eine Stärkung der nationalen Cybersicherheitsarchitektur und durch einen verstärkten Schutz der Wirtschaft und der öffentlichen Verwaltung entgegengewirkt werden.
    - Im Rahmen dieses Gesetzgebungsverfahrens können nicht alle notwendigen Maßnahmen ergriffen werden, z.B. benötigen
        - Die Neuaufstellung der Gefahrenabwehr im Cyberraum und
        - Die Positionierung des BSI als Zentralstelle im Bund-Länder-Verhältnis
    - Änderungen des Grundgesetzes und damit einen weitergehenden gesetzgeberischen Ansatz, aber
    - NIS2 kann für die harmonisierte Erhöhung des Schutzniveaus in der Wirtschaft und der Bundesverwaltung genutzt werden.
- Dazu müssen allerdings **folgende Defizite des aktuellen Entwurfs** ausgeräumt werden:
- In §29 wird durch die Einschränkung des Anwendungsbereiches in Absatz (1) sowie die Ausnahmen von den Regelungen für besonders wichtige Einrichtungen **für den Großteil der Bundesbehörden** in §29(2) **das Harmonisierungs- und Sicherheitsziel von NIS2 verfehlt**. Dies hat zur Folge,
    - Dass in der Bundesverwaltung verschiedene Sicherheitsniveaus entstehen,
    - Das Sicherheitsniveau hinter das mit dem Umsetzungsplan Bund 2.0 erreichte Niveau zurückfällt,
    - Der IT-Grundschutz entwertet und nicht einmal mehr durch das BSI als Bundesbehörde beachtet werden muss,
    - Der Bund für sich selbst geringerer Anforderungen vorsieht als die Beschlüsse des IT-Planungsrates für die Länder,
    - Den Anforderungen des Geheimschutzes für die Erreichung auch nur des niedrigsten Schutzniveaus „Verschlusssache nur für den Dienstgebrauch“ im größten Teil der Bundesverwaltung nicht mehr gegeben sind,
    - Der Anschluss an die Netzinfrastrukturen des Bundes unmöglich wird und
    - IT-Dienstleistungen für schützenswerte Dienste von den IT-Dienstleistern des Bundes nicht mehr bezogen werden können.
- Die als Folge der Ausnahmen des §29 eingeführten Vorgaben des BSI im Absatz §44(1) laufen insoweit ins Leere, dass entsprechende Mindeststandards aktuell nur in einem geringen Maße und für wenige Anwendungsbereiche existieren, da alle Anforderungen bisher auf dem IT-Grundschutz aufsetzten.
- Zum Absatz §29(3) gilt hinsichtlich der zusätzlichen Ausnahmen für das Auswärtige Amt und das BMVg entsprechendes, siehe oben.

- Absatz §44(1) zu Mindeststandards in der Bundesverwaltung entspricht dem §8(1) des BSIG in der derzeit geltenden Fassung. Im Zuge der vorgeschlagenen Änderung des §29 sollten die Mindeststandards auf den jetzt geltenden Stand zurückgeführt oder aber abgeschafft und in einen novellierten IT-Grundschutz integriert werden.
- Die **Verbindlichkeit des IT-Grundschutzes für die öffentliche Verwaltung** ist im Zuge der NIS2-Umsetzung richtig, sollte aber wie mehrfach dargelegt für die gesamte (Bundes-)Verwaltung gelten.
  Die in §44(2) genutzten **Formulierungen zum IT-Grundschutzes entsprechen nicht dem wissenschaftlichen und fachlichen Stand**. Im Zuge der oben vorgeschlagenen Änderungen des §29 sollten die Formulierungen überarbeitet werden.
- **Die Einführung des Koordinators für die Informationssicherheit des Bundes ist ein richtiger Schritt, die reine Bestellung in §48 greift aber zu kurz.** Wie bereits oben ausgeführt kann der Koordinator aber nur dann erfolgreich seine Aufgabe wahrnehmen, wenn seine Aufgaben und Befugnisse im Gesetz ausgeführt werden. Insofern sollten die §§49 und 50 des dritten Entwurfs wieder aufgenommen werden (siehe Anlage).
- Darüber hinaus kann ein Koordinator (oder besser Informationssicherheitsbeauftragter nur dann erfolgreich die Cyber- und Informationssicherheit in Deutschland gestalten und umsetzen, wenn er dazu
  - Auf Augenhöhe mit den Ressorts der Bundesregierung agiert,
  - die Spitze des Informationssicherheitsmanagements der Bundesverwaltung bildet (etwa im IT-Rat des Bundes) und die
  - Budgethoheit für Cyber- und Informationssicherheit im Bund besitzt.
- Alle Maßnahmen der NIS2-Umsetzung müssen, wo irgend möglich und sinnvoll mit der Entwicklung und Einführung entsprechender digitaler Werkzeuge, z.B. im Meldewesen, Informationssicherheits- und Risikomanagement einhergehen. Nur eine Digitalisierung der Informationssicherheit wird Informationssicherheit in der Digitalisierung ermöglichen.
- **Schließlich muss für die Ressorts, Bundesbehörden und das BSI eine angemessene Haushaltsausstattung bereitgestellt werden.** Insbesondere können die notwendigen Maßnahmen in der Zusammenarbeit mit der Wirtschaft durch das BSI nur erfolgen, wenn ein entsprechender Personalaufwuchs gewährt wird. Gleiches gilt für die personelle Aufstellung der Bundesbehörden im Informationssicherheitsmanagement.
  Finanzmittel sind vor allem für die Digitalisierung der Informationssicherheit erforderlich.

Schlussfolgerungen für mögliche weitere Erörterungen im Deutschen Bundestag

Der Deutsche Bundestag, der Innenausschuss und auch der Ausschuss für Digitales könnten sich in der weiteren Diskussion des NIS2UMsuCG aus meiner Sicht daher mit folgenden Themen auseinandersetzen:

- Im §29 Streichung aller Einschränkungen zum Anwendungsbereich in Absatz (1). Änderung des §29(2) zur vollumfänglichen Unterstellung der Bundesverwaltung unter die Regelungen für besonders wichtige Einrichtungen.
- Überführung des §41 BSIG-E alias „§9b“ in das KRITIS-DG und Novellierung.
- Anpassung des §44(2) zur Verbindlichkeit des IT-Grundschutzes für die Bundesverwaltung
- Stärkung der Rolle des Koordinators für Informationssicherheit des Bundes mindestens durch Aufnahme der §§49 und 50 des dritten Entwurfs des NIS2UMsuCG
- Bereitstellung von Haushaltsmitteln und vor allem Personal für die Umsetzung von NIS2 in den Haushalten der Jahre 2025ff.

Anlage

§ 49 **Aufgaben des Koordinators**

Dem Koordinator oder der Koordinatorin für Informationssicherheit obliegt die zentrale Koordinierung des Informationssicherheitsmanagements des Bundes. Zu diesem Zweck erhält er unter Berücksichtigung der Ergebnisse der Kontrollen nach § 7 einen Überblick über die Informationssicherheitslage in der Bundesverwaltung. Er oder sie koordiniert die Erstellung und Aktualisierung von Informationssicherheitsleitlinien des Bundes und unter-stützt die Ressorts bei der Umsetzung der Vorgaben zur Informationssicherheit. Dabei wirkt er oder sie auf ein angemessenes Verhältnis zwischen dem Einsatz von Informationstechnik und Informationssicherheit hin. Bei der Aktualisierung der Informationssicherheitsleitlinien des Bundes berücksichtigt er oder sie die Erfahrungen aus der Unterstützung der Ressorts.

§ 50 **Befugnisse des Koordinators**

(1) Zur Wahrnehmung der Aufgaben nach § 49 informieren die Ressorts den Koordinator oder die Koordinatorin für Informationssicherheit über alle Gesetzes-, Verordnungs- und sonstigen wichtigen Vorhaben, soweit sie Fragen der Informationssicherheit berühren. Er oder sie kann der Bundesregierung Vorschläge machen und Stellungnahmen zuleiten. Die Ressorts unterstützen den Koordinator oder die Koordinatorin bei der Erfüllung seiner oder ihrer Aufgaben.

(2) Zur Wahrnehmung seiner oder ihrer Aufgaben hat der Koordinator oder die Koordinatorin ein direktes Vortragsrecht vor dem Ausschuss für Inneres und Heimat und dem Haushaltsausschuss des Deutschen Bundestages zu allen Themen der Informationssicherheit in Einrichtungen der Bundesverwaltung.

(3) Der Koordinator oder die Koordinatorin kann im Benehmen mit dem oder der Informationssicherheitsbeauftragten des jeweils zuständigen Ressorts Einrichtungen anweisen, innerhalb von drei Monaten nach der Vorlage der Ergebnisse von Kontrollen gemäß § 7 ein Sofortprogramm vorzulegen, das die Einhaltung der Anforderungen innerhalb einer angemessenen Umsetzungsfrist sichert.