20. Wahlperiode

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Wortprotokoll
der 90. Sitzung

Ausschuss für Inneres und Heimat
Berlin, den 4. November 2024, 11:00 Uhr
Konrad-Adenauer-Str. 1, Berlin 10557
Paul-Löbe-Haus, Raum E 800

Vorsitz: Petra Pau, MdB

Tagesordnung - Öffentliche Anhörung

Tagesordnungspunkt 1 **Seite 5**

Gesetzentwurf der Bundesregierung

**Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie
und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung
(NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz)**

BT-Drucksache 20/13184

Federführend:
Ausschuss für Inneres und Heimat

Mitberatend:
Wirtschaftsausschuss
Ausschuss für Arbeit und Soziales
Verteidigungsausschuss
Ausschuss für Digitales
Ausschuss für Klimaschutz und Energie
Haushaltsausschuss (mb und § 96 GO)

Berichterstatter/in:
Abg. Daniel Baldy [SPD]
Abg. Marc Henrichmann [CDU/CSU]
Abg. Dr. Konstantin von Notz [BÜNDNIS 90/DIE GRÜNEN]
Abg. Manuel Höferlin [FDP]
Abg. Steffen Janich [AfD]
Abg. Martina Renner [Die Linke]

Inhaltsverzeichnis

Stellungnahmen der Sachverständigen

Unangeforderte Stellungnahmen

Dem Ausschuss sind die vorliegenden Stellungnahmen teilweise in nicht barrierefreier Form zugeleitet worden.

Anwesende Mitglieder des Ausschusses

Fraktion/Gruppe	Ordentliche Mitglieder	Stellvertretende Mitglieder
SPD	Baldy, Daniel Hartmann, Sebastian	
CDU/CSU	Henrichmann, Marc Sekmen, Melis Throm, Alexander	
BÜNDNIS 90/DIE GRÜNEN	Khan, Misbah Notz, Dr. Konstantin von	
FDP	Höferlin, Manuel	
AfD	Janich, Steffen	
Die Linke	Pau, Petra	
BSW		
fraktionslos		

Liste der Sachverständigen

Öffentliche Anhörung am Montag, 4. November 2024, 11.00 Uhr
„NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz“

Boris Eisengräber[2)]
Leiter Cyber Security - Schwarz Digits, Neckarsulm

Dr. Sven Herpig[4)]
Lead Cybersecurity Policy and Resilience interface – Tech analysis and policy ideas for Europe e.V.

Prof. Dr. Dennis-Kenji Kipker[3)]
Universität Bremen

Prof. Timo Kob[2)]
HiSolutions AG, Berlin

Andreas Könen[2)]
Senior Fellow
Brandenburgisches Institut für Gesellschaft und Sicherheit (BIGS) gGmbH, Potsdam

Felix Kuhlenkamp[1)],
Bitkom e. V., Berlin

Claudia Plattner[3)]
Präsidentin - Bundesamt für Sicherheit in der Informationstechnik, Bonn

Prof. Dr. Haya Schulmann[1)]
Johann Wolfgang Goethe-Universität Frankfurt am Main und ATHENE

---

1) Vorschlag: Fraktion der SPD
2) Vorschlag: Fraktion der CDU/CSU
3) Vorschlag: Fraktion der BÜNDNIS 90/DIE GRÜNEN
4) Vorschlag: Fraktion der FDP

Einziger Tagesordnungspunkt

Gesetzentwurf der Bundesregierung

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

BT-Drucksache 20/13184

AmtVors. **Petra Pau** (Die Linke): Guten Tag, meine sehr verehrten Damen und Herren! Ich eröffne die 90. Sitzung des Ausschusses für Inneres und Heimat und begrüße Sie alle recht herzlich. Mein Name ist Petra Pau. Ich bin die amtierende Vorsitzende des Ausschusses für Inneres und Heimat und werde die öffentliche Anhörung der Sachverständigen leiten. Ich danke Ihnen, sehr geehrte Sachverständige, dass Sie unserer Einladung nachgekommen sind und uns mit Ihrer Expertise zur Verfügung stehen, um die Fragen der Kolleginnen und Kollegen aus dem Ausschuss für Inneres und Heimat und der mitberatenen Ausschüsse zu beantworten. Ich begrüße daher zunächst die von den Fraktionen benannten Sachverständigen, Herrn Boris Eisengräber, Herrn Dr. Sven Herpig, Herrn Prof. Dr. Dennis Kenji-Kipker, Herr Prof. Timo Kob, Herrn Andreas Könen, Herrn Felix Kuhlenkamp, Frau Claudia Plattner und Frau Prof. Dr. Haya Schulmann. Der Sachverständige Prof. Dr. Marian Margraf kann krankheitsbedingt nicht teilnehmen, hat aber eine schriftliche Stellungnahme eingereicht. Für die Bundesregierung darf ich den Herrn Parlamentarischen Staatssekretär Johann Saathoff aus dem Bundesministerium des Innern und für Heimat willkommen heißen.

Die Sitzung wird live auf der Homepage des Deutschen Bundestages übertragen und ab morgen über die Mediathek für die Öffentlichkeit zum Abruf bereitgestellt. Wir hatten schriftliche Stellungnahmen erbeten. Für die eingegangenen Stellungnahmen bedanke ich mich bei den Sachverständigen. Sie sind an alle Ausschussmitglieder verteilt worden und werden dem Protokoll der Sitzung beigefügt. Ich gehe davon aus, dass Ihr Einverständnis zur Durchführung der öffentlichen Anhörung auch die Aufnahme der Stellungnahmen in eine Gesamtdrucksache umfasst. Von der heutigen Anhörung wird ein Wortprotokoll erstellt und Ihnen zur Korrektur übersandt. Im Anschreiben werden Ihnen Details zur Behandlung mitgeteilt. Die Gesamtdrucksache, bestehend aus Protokoll- und schriftlichen Stellungnahmen, wird im Übrigen auch ins Internet eingestellt. Für die Anhörung ist die Zeit von 11 bis 13 Uhr vorgesehen. Ich werde gleich jedem Sachverständigen die Gelegenheit geben, einleitend drei Minuten seine Position darzustellen. Ich bitte tatsächlich, sich auf diese drei Minuten zu konzentrieren. Wie gesagt, Ihre schriftlichen Stellungnahmen wurden verteilt. Nach den Eingangsstatements werden wir orientiert an Fraktionsrunden mit der Befragung der Sachverständigen beginnen. Ich bitte, dass die Fragestellenden diejenigen Sachverständigen ausdrücklich benennen, an die Sie die Frage richten wollen. Zu den Frageregeln gilt: In den Fraktionsrunden kann jede Fragestellerin und jeder Fragesteller entweder zwei Fragen an eine Sachverständige bzw. einen Sachverständigen oder je eine Frage an zwei Sachverständige richten. Für die Fragen gilt eine Zwei-Minuten-Zeitbegrenzung. Die Auskunftsperson antwortet unmittelbar auf die Frage. Für die Antwort auf jede Frage stehen ebenfalls zwei Minuten zur Verfügung. Nach der zweiten Fraktionsrunde werde ich angesichts der fortgeschrittenen Zeit situativ entscheiden, ob das Zeitfenster weiterhin zwei oder nur noch eine Frage zulässt. Wenn Sie damit einverstanden sind, werden wir so verfahren. Bevor ich jetzt den ersten Sachverständigen ums Wort bitte, nur erklärend die Anmerkung, dass der Kollege Höferlin noch in der Anreise ist. Er wird sich evtl. hier gleich noch digital zuschalten. Ich hoffe jedenfalls, dass er dann zur Fragerunde auch hier anwesend ist. Entsprechend der alphabetischen Reihenfolge darf ich dann Herrn Eisengräber um seine Eingangsstellungnahme bitten.

SV **Boris Eisengräber** (Schwarz Digits)**:** Guten Tag, Frau Vorsitzende, meine sehr geehrten Damen und Herren Abgeordnete. Zunächst vielen Dank für die Möglichkeit, heute zum Gesetzentwurf Stellung nehmen zu können. Ich spreche als Vertreter der Schwarz Digits, der IT- und Digitalsparte der Unternehmen der Schwarz Gruppe. Ich bin hier unter anderem für die Umsetzung der Vorgaben des aktuellen BSI-Gesetzes (Gesetz über das Bundesamt für Sicherheit in der Informationstechnik) sowie des zukünftigen NIS-2- Umsetzungs- und Cybersicherheitsstärkungsgesetzes zuständig. Wir sind schon heute in Teilen kritische Infrastruktur. Die Zusammenarbeit mit dem BSI erleben wir hierbei als sehr positiv und als wichtigen Erfolgsfaktor für die Verbesserung der

Cybersicherheit in Deutschland. Aufgrund der Abhängigkeit als Neuunternehmen von funktionierenden Lieferketten, Infrastruktur und Behörden ist die übergreifende Definition und Durchsetzung eines Mindestsicherheitsniveaus wie in der NIS-2-Richtlinie begrüßenswert und notwendig. Die geforderten Risikomanagementmaßnahmen folgen Best Practices und sollten aus unserer Sicht ohnehin aus Eigeninteresse zum Schutz gegen Cyberbedrohungen getroffen werden.

Wir plädieren, die Anforderungen des NIS-2 Umsetzungs- und Cybersicherheitsstärkungsgesetzes und des KRITIS-Dachgesetzes (Gesetz zur Umsetzung der Richtlinie (EU) 2022/2557 und zur Stärkung der Resilienz kritischer Anlagen) aufeinander abzustimmen. Die in § 32 BSI-Gesetzentwurf definierte gemeinsame Meldestelle des BSI sowie des BBK (Bundesamt für Bevölkerungsschutz und Katastrophenhilfe) ist hierbei eine positive Entwicklung. Unterschiedliche Umsetzungen der NIS-2-Richtlinie in den Mitgliedstaaten werden für EU-weit agierende Unternehmen eine Herausforderung darstellen und effektive Reaktionen auf Cyberangriffe erschweren. Ein möglicher Lösungsansatz ist, Nachweis-, Melde- und Registrierungspflichten auf den Mitgliedsstaat zu beschränken, in dem die jeweilige IT-Infrastruktur betrieben wird. Neben dem Fokus auf reaktive Risikomanagementmaßnahmen ist auch die Berücksichtigung von präventiven Sicherheitsmaßnahmen wichtig und hervorzuheben, bei weiteren Konkretisierungen ist zu beachten, dass die Technologieoffenheit gewahrt bleibt. Die Etablierung eines angemessenen Cybersicherheitsniveaus ist eine gesamtgesellschaftliche Aufgabe, bei der der Staat eine Vorbildfunktion einnimmt. Zur Verbesserung der Cybersicherheit im öffentlichen Sektor gehört neben der Stärkung des Bundesamtes für Sicherheit in der Informationstechnik und weiterer Sicherheitsfunktionen auch die Modernisierung der IT-Infrastruktur nach Stand der Technik und der Nutzung von Lösungen zur Stärkung der digitalen Souveränität sowie der Bereitstellung des hierfür erforderlichen Budgets bei Bund, Ländern und Kommunen. Für weitere Details darf ich auf die umfangreiche schriftliche Stellungnahme verweisen. Vielen Dank.

AmtVors. **Petra Pau** (Die Linke): Ich danke Ihnen. Wir gehen dann weiter zu Herrn Dr. Sven Herpig.

SV **Dr. Sven Herpig** (interface): Vielen Dank. Sehr geehrte Frau Vorsitzende, sehr geehrte Ausschussmitglieder, Abgeordnete, Mitarbeitende, die mit beiden Beinen fest auf dem Boden unserer freiheitlich-demokratischen Grundordnung stehen, sehr geehrter Herr Staatssekretär, sehr geehrte interessierte Öffentlichkeit, ich möchte vier Aspekte meiner schriftlichen Stellungnahme hervorheben.

Erstens: Die Umsetzung der NIS-2-Richtlinie gibt uns die Möglichkeit einer harmonisierten IT-Sicherheitsregulierung von Bund und Ländern. Die Chance wird im aktuellen Gesetzentwurf vertan, vor allem deswegen, weil ein wichtiger Punkt des Koalitionsvertrags bisher nicht umgesetzt werden konnte. Dort heißt es, zur Erinnerung: „Wir leiten einen strukturellen Umbau der IT-Sicherheitsarchitektur ein, stellen das BSI unabhängiger auf und bauen es als zentrale Stelle im Bereich IT-Sicherheit aus.“ Deutschland bleibt jetzt allerdings neben einer fragmentierten IT-Sicherheitsarchitektur und einer fragmentierten Cybersicherheitsstrategie auch noch bei seiner fragmentierten IT-Sicherheitsregulierung. Das ist weder effektiv noch effizient oder im Sinne der Cybersicherheit dieses Landes.

Zweitens: Die Umsetzung der NIS-2-Richtlinie sieht die Notwendigkeit einer operativ-unabhängigen Stelle. Auch dieser Aspekt wird im aktuellen Gesetzentwurf nicht ausreichend berücksichtigt. Und das, obwohl es im Koalitionsvertrag heißt, Zitat: „Wir […] stellen das BSI unabhängiger auf.“ Der Diskurs um eine größere Unabhängigkeit des BSI dauert bereits seit Jahren an. Es gibt mittlerweile viele ausgearbeitete Vorschläge dazu, wie das geschehen kann. Dass der Gesetzentwurf keinen einzigen dieser Vorschläge aufgreift oder einen anderen Vorschlag macht, ist wenig nachvollziehbar.

Drittens: Die teils weitreichenden Ausnahmeregelungen für Einrichtungen der Bundesverwaltung sind fachlich fragwürdig. Und das waren sie schon, als wir analoge Regelungen in der Debatte um das IT-Sicherheitsgesetz 2.0 diskutiert hatten. Als jemand, der mal in der Stabsstelle IT-Sicherheit des Auswärtigen Amtes gearbeitet hat, verstehe ich den Bedarf von Ausnahmen bei komplexen IT-Infrastrukturen. Wenn ich mich jedoch jetzt in meine Rolle von damals hineinversetze, dann würde ich mich sicherlich nicht gegen mehr Regulierung wehren. Ich rege an, sich noch einmal genauer mit den Fortschritten von IT-Sicherheit

im Bund auf Basis des Umsetzungsplans Bund vertraut zu machen und daraus abzuleiten, ob evtl. einzelne Bereiche und Einrichtungen wirklich von diesen sinnvollen IT-Sicherheitsregelungen ausgenommen werden sollten.

Viertens: Viele Staaten betrachten Schwachstellen mittlerweile als strategische Ressource und den Umgang damit als relevant für die nationale Sicherheit. Mehrere Länder, darunter die Vereinigten Staaten, Australien, die Volksrepublik China und die Niederlande haben daher umfassende Policies zum Umgang mit Schwachstellen implementiert. In Deutschland macht jeder staatliche Akteur mit Informationen zu Schwachstellen das, was ihm sein gesetzlicher Rahmen erlaubt, ohne dass es hier eine übergeordnete Strategie gibt. Das aktuelle Modell folgt den Partikularinteressen der einzelnen Sicherheitsbehörden mit einem Mindestgrad an Transparenz und Kontrolle. Für Externe, also Mitarbeitende anderer Behörden oder Sicherheitsforscher, schafft es Misstrauen und rechtliche Unsicherheiten und damit negative Anreize, Schwachstellen zu melden und somit auf mehr Cybersicherheit hinzuwirken. Die Umsetzung der NIS-2-Richtlinie gibt uns die Möglichkeit, ein umfassendes staatliches Schwachstellenmanagement nach deutscher Lesart einzuführen. Flankiert wird diese NIS-2-Richtlinie auch hier vom Koalitionsvertrag, in dem es heißt: „Wir führen […] ein wirksames Schwachstellenmanagement mit dem Ziel, Sicherheitslücken zu schließen, […] ein“. Während der vorliegende Gesetzesentwurf für einzelne Regelungen zum Umgang mit Schwachstellen und zu bestehenden Prozessen ergänzt, ergibt sich daraus kein umfassendes staatliches Schwachstellenmanagement, sondern lediglich mehr Komplexität, und Komplexität ist bekanntlich der Feind von IT-Sicherheit. Dass wir seit über sieben Jahren daran scheitern, ein ressortübergreifendes staatliches Schwachstellenmanagement zu implementieren, ist nichts weniger als enttäuschend.

Abschließend möchte ich noch meine Verwunderung darüber ausdrücken, dass trotz Berührung ihres Zuständigkeitsbereichs die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) nicht durch den Ausschuss geladen wurde.

AmtVors. **Petra Pau** (Die Linke): Danke. Wir machen weiter mit Prof. Dr. Kipker.

SV **Prof. Dr. Dennis-Kenji Kipker** (Universität Bremen): Sehr geehrte Vorsitzende, sehr geehrte Ausschussmitglieder, sehr geehrte Damen und Herren! Ich bedanke mich für die Möglichkeit, hier heute Stellung zum Entwurf des NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetzes nehmen zu können. Gemessen an der Tatsache, dass die Umsetzung von NIS-2 in Deutschland schon seit mittlerweile fast zwei Jahren möglich ist und angegangen wird, enthält der vorgelegte Entwurf leider noch zu viele Schwächen und Unklarheiten, teilweise auch Maßgaben, die der Erhöhung des allgemeinen Cybersicherheitsniveaus nicht förderlich sind. Zu vermissen ist ebenfalls eine Vereinheitlichung der Systematik des nationalen Cybersicherheitsrechts, die zwischen bereichsspezifischen und allgemeinen Vorgaben und der Cybersicherheit in Bund und Ländern unterscheidet. Denn letztlich verlangt NIS-2 nichts anderes, als dass selbst in einem föderalen Deutschland einheitliche Cybersicherheitsstandards definiert werden. Aufgrund der nach wie vor bestehenden Zersplitterung von Vorgaben, verteilt auf unterschiedliche regulatorische Ebenen mit unterschiedlicher Verbindlichkeit und verschiedener inhaltlicher Dichte, sind wir zurzeit noch weit von einer einheitlichen Umsetzung entfernt.

Hauptkritikpunkte betreffen dabei die nach wie vor im nationalen Verwaltungsgefüge unklare Rolle des BSI, die nicht angetastet wurde, obwohl das BSI nicht nur in seiner Rolle als Zentralstelle für Cybersicherheit einen weiteren Ausbau erfahren soll, sondern mit NIS-2 auch zahlreiche weitere Befugnisse erhalten wird. Bereits ebenso mehrfach kritisierte begriffliche Schwächen, die sich bereits im geltenden Recht wiederfinden, werden noch nicht ausgeräumt. Dies ist für den richtigen und rechtssicheren Umgang mit den Vorschriften durch die Betroffenen jedoch essentiell. Ganz zentral ist überdies die gesetzlich angeordnete Umsetzung von IT-Sicherheitsmaßnahmen nach NIS-2 und § 30-BSI-Gesetzentwurf. Hier wird nahezu eins zu eins auf den NIS-2-Maßnahmenkatalog verwiesen, was bei betroffenen Einrichtungen jedoch zur Unsicherheit darüber führt, welche Maßnahmen einzeln zu realisieren sind, ob diese überhaupt in den konkreten betrieblichen Anwendungskontext passen.

Durch die pauschale Anordnung der Verwendung von Systemen zur Angriffserkennung und weiteren Einzelmaßnahmen gerät zunehmend außer

Fokus, dass Cybersicherheit eine Managementaufgabe ist, die sich an eine individuelle Risikobewertung anschließt und deshalb zunächst nichts mit einzelnen Produkten und Insellösungen zur Cybersicherheit zu tun hat. Diese Unsicherheit für betroffene Einrichtungen zieht sich bedauerlicherweise durch den gesamten Gesetzentwurf und somit auf die Registrierung, das Meldewesen, die Anforderungen an Dokumentation und Nachweise, die Geschäftsleiterverantwortlichkeit sowie die Schaffung von betrieblicher Awareness. Über den Bereich betroffener Privatunternehmen hinausgehend finden sich überdies auch im öffentlichen Teil des Gesetzesvorschlags weitere und auch systematische Schwächen, die an die Definition von Einrichtungen der Bundesverwaltung und an die künftige Rolle des CISO Bund (CISO: Chief Information Security Officer), die weiterhin undefiniert im Raum steht, anknüpfen.

Im Hinblick auf den Datenschutz enthält der Entwurf außerdem weitere erhebliche nennenswerte Schwächen, die teils sogar unionsrechtswidrig sein dürften, zum Beispiel die Anforderung, nur offensichtliche Datenschutzverletzungen infolge eines Cybersicherheitsvorfalls an die Datenschutzaufsicht zu melden und wie die Befugnisse von BSI und BFDI auch künftig klar voneinander abzugrenzen sein sollen. In meiner Stellungnahme hatte ich überdies angemerkt, dass die Einbeziehung der BfDI in den weiteren Gesetzgebungsprozess ratsam wäre, was mit Stellungnahme von heute nun auch geschehen ist.
Vielen Dank.

AmtVors. **Petra Pau** (Die Linke): Ich danke Ihnen. Das Wort geht an Prof. Kob.

SV **Prof. Timo Kob** (HiSolutions): Sehr geehrte Frau Vorsitzende, sehr geehrte Ausschussmitglieder, sehr geehrte Damen und Herren. Ich werde in den drei Minuten nicht auf Details eingehen, sondern mir geht es eher darum, den sense of urgency zu steigern, vielleicht durchaus auch mit der Absicht, etwas provokativ zu sein. Ich schaue mir deswegen die heutige Situation aus Sicht des Angreifers an. Da haben wir die erste Ebene, wo wir auf Schwachstellen schauen, das ist die Technik. Da haben wir die typischen Schwachstellen: Passworte, zu viele Rechte, veraltete Software. Wir haben eine zweite Dimension, das ist die Organisation. Da geht es um fehlende Verantwortlichkeiten, unklare Prozesse, Awareness bei Mitarbeitern und Geschäftsführern. Wenn ich aus den beiden Blickwinkeln schaue, kann ich sagen, dass das im Gesetz gut adressiert ist. Es ist überall im Detail noch zu klären, aber wir sind da auf dem richtigen Weg. Das Problem ist, wir sind jetzt schon verzögert in der Einführung. Wir sehen aber auch, dass das in bisher regulierten Branchen, wie eben bei den Finanzdiensten, ja auch gut funktioniert. Die Häuser sind sicherer als diejenigen, die nicht reguliert sind. Von daher müssen wir dazu kommen, dies schnellstens zu implementieren. Aber es gibt noch eine dritte Ebene. Die dritte Ebene ist dann Staat und Gesellschaft. Bevor die Techniker und die Geschäftsführer Fehler machen könnten, sind wir jetzt in dem Bereich, wo die Politiker die Fehler machen können. Wenn ich da nach den Top 3 der Schwachstellen gefragt werde, dann wird es jetzt vielleicht einen Aufschrei geben, aber dann heißen die für mich: Föderalismus und Ressortunabhängigkeit – in der Form, wie sie jetzt betrieben werden und – eben schlecht priorisierte Haushaltsmittel. Was das dann bedeutet, das ist natürlich ein Thema, das viel größer ist als NIS-2, aber die Chance in diesem Gesetz wäre gewesen, den ersten Schritt in die richtige Richtung zu gehen. Das fehlt völlig im Gesetz. Im Gegenteil, es ist teilweise eher ein Rückschritt, Thema Ausnahmen, die für nachgeordnete Behörden gemacht werden.

Wenn wir sagen, dass Ketten so stark sind wie das schwächste Glied, dann haben wir eher ein Cyber-Schwächungsgesetz. Das hat nichts damit zu tun, dass ich jetzt eingekreist bin von denen, die heute noch verantwortlich sind und die bis gestern dafür verantwortlich waren – weniger war das BMI verantwortlich als andere Ministerien, die aus der Außenwahrnehmung eher wie in einem Handel gesagt haben, ich stimme dem zu, wenn ich folgende Ausnahmen bekomme. Ich will das ganze mal bildlich machen, auch wenn mir die Zeit wegläuft. Sie kennen wahrscheinlich alle den Dodo, den Vogel, der ausgestorben ist, weil er sich nicht mehr an neue Gefährdungen anpassen konnte. Wenn ich das mal übertrage: Wer glaubt, dass Cyber-Gefährdungen sich genauso managen lassen, wie ein überlaufender Fluss, nämlich am besten von einem Landrat, und nicht sieht, dass wir ein einheitliches Niveau brauchen, dass wir einheitliche Vorgaben brauchen, dass wir einheitliche Verantwortlichkeiten brauchen, der wird als Cyber-Dodo enden. Wer nicht sieht, dass Ausnahmen für Ministerien nicht sinnvoll sind, dass reduzierte Anforderungen für nachgeordnete Behörden –

Außenministerien sind ja nicht die einzigen, für die es Ausnahmen gibt –, dass das kontraproduktiv ist, wenn wir kein einheitliches Niveau haben, der wird als Cyber-Dodo enden. Wer den Bundes-CISO einführen will, aber ohne wirkliche Durchgriffsrechte, weil man dann eigene Befugnisse abgeben müsste, der wird als Cyber-Dodo enden. Wer dem BSI nur eingeschränkte Rechte gibt, Stichwort „Schwachstellen-Scan“, die teilweise sogar Privatpersonen möglich wären, der wird ebenfalls als Cyber-Dodo enden. Und jetzt gehe ich mal einen Schritt weiter. Wer als großes Bundesland glaubt, bloß, – –

AmtVors. **Petra Pau** (Die Linke): Sie müssen zum Ende kommen.

SV **Prof. Timo Kob** (HiSolutions): – – weil man es kurzfristig besser machen kann, mache ich es lieber allein als der Bund, der wird ebenfalls seine Probleme haben. Das mag kurzfristig sein, aber man muss immer denken, wenn man größer ist als das Saarland, kann man immer noch kleiner sein als Russland. Wer in der Prävention Geld spart, der wird am Ende teuer bezahlen. Von daher: Schnellstens das Gesetz einführen, aber bitte diese Änderung, diese Schwächung auf staatlicher Seite ändern.

AmtVors. **Petra Pau** (Die Linke): Danke, das Wort geht an Herrn Könen.

SV **Andreas Könen** (BIGS)**:** Ich möchte mich ebenfalls zunächst für die Einladung in die Sachverständigenanhörung bedanken. Meine Person dürfte hinlänglich bekannt sein.

Wenn ich noch einmal da starte, wo es losgegangen ist, nämlich bei NIS-2 selbst und der europäischen Richtlinie, dann muss man ganz deutlich sagen, Ziel der europäischen Richtlinie war eine wirklich sehr weitgehende, breite Harmonisierung des Informationssicherheitsrechts in der Europäischen Union und vor allen Dingen ein Schutz der kritischen Infrastrukturen und der Unternehmen, die für unsere Volkswirtschaften relevant sind. Dieses Harmonisierungsziel, muss man leider sagen, ist auch in der NIS-2-Richtlinie selbst in Teilen nicht völlig erreicht worden. Etwa das, was wir hier im konkreten Umsetzungsgesetz wiederfinden, was die föderale Ebene angeht und was tatsächlich dann auch die Regulierung der Bundesbehörden angeht, ist tatsächlich auch Ausdruck der Schwächen, die in NIS-2 schon mitenthalten sind. Dies dürfte mein erster Punkt sein.

Ich sehe vor allen Dingen dort, wo es um die Regulierung der Bundesbehörden geht, deutliche Schwächen, indem unterschieden wird zwischen den Ministerien und dem Kanzleramt auf der einen Seite, die höhere Anforderungen erfüllen müssen und den Bundesbehörden, die tatsächlich unter den Regulierungsstand zurückfallen, der bereits mit dem Umsetzungsplan BUND 2.0 erreicht wurde. Das ist ein falsches Signal, vor allen Dingen auch an die Wirtschaft, die jetzt viel breiter reguliert wird. Hier wäre sicher Gelegenheit zur Nacharbeit gegeben. Vor allen Dingen ist es so, dass sich die Frage stellt, wie Netze des Bundes, IT-Dienstleister des Bundes und auch der Anschluss an den Geheimschutz in einer solchen Form gelingen kann.

Der IT-Grundschutz selbst ist ebenfalls im Gesetz nicht in adäquater Weise behandelt. Dort werden im Gegensatz zu dem, was das BSI eigentlich werden soll, nämlich fachlich unabhängiger und unabhängig in fachlicher Form, sehr konkrete Bedingungen getroffen, wie IT-Grundschutz weiterzuentwickeln und einzusetzen ist. Das finde ich allein fachlich nicht adäquat. Darüber hinaus ist es so, dass, wie bereits von einigen Vorrednern erwähnt, die Position eines CISO des Bundes eingerichtet werden sollte. Er muss konkrete, klar definierte Befugnisse haben, die sich vor allen Dingen im Controlling bei IT-Projekten und auch bei den Finanzen äußern. Sie wissen, ich persönlich bin der Meinung, dass es ein Ansprechpartner auf Augenhöhe für die Ressorts sein muss, also ein Staatssekretär in einem der Ministerien, und er muss Budgetverantwortung haben.

Damit möchte ich auch direkt überleiten zu meinem Abschlussplädoyer. Bitte stärken Sie das BSI durch fachlich unabhängigere Aufstellung, durch verbesserte finanzielle und personelle Aufstellung und richten Sie einen CISO des Bundes ein, der tatsächlich auch eine Budgethoheit für Cybersicherheit besitzt. Danke.

AmtVors. **Petra Pau** (Die Linke): Vielen Dank. Das Wort hat Herr Kuhlenkamp.

SV **Felix Kuhlenkamp** (Bitkom)**:** Vielen Dank auch von meiner Seite, dass ich heute als Vertreter des Bitkom zum NIS2-Umsetzungs- und

Cybersicherheitsstärkungsgesetz Stellung nehmen darf.

Unsere Wirtschaftsschutzstudie zeigt, im letzten Jahr entstand in deutschen Unternehmen ein Rekordschaden von 178 Milliarden Euro allein durch Cyberangriffe. Die Tendenz ist steigend. Angesichts dieser Bedrohungslage begrüßen wir die Ziele von NIS-2 für ein einheitliches Cybersicherheitsniveau in der EU. Gleichzeitig stehen viele Unternehmen durch NIS-2 und andere digitalpolitische Gesetze jedoch vor einer großen Umsetzungswelle. Für eine effiziente Anwendung in der Praxis braucht es daher eine koordinierte und harmonisierte Implementierung. Dabei schließe ich mich den hier bereits angebrachten Punkten an, insbesondere im Hinblick auf das Schwachstellenmanagement, die Rolle des BSI und den Bundes-CISO. Ich möchte auch drei weitere zentrale Punkte hervorheben, die für die deutsche Wirtschaft von Bedeutung sind.

Erstens: Die Kommunikation und Unterstützung für regulierte Einrichtungen ist noch verbesserungswürdig. In Ländern wie Lettland und Italien werden die betroffenen Unternehmen aktiv von der Regierung informiert. In Deutschland müssen hingegen 30 000 Unternehmen selbst herausfinden, dass sie von der NIS-2-Richtlinie betroffen sind. Die Frage lautet daher, warum informiert der deutsche Staat hier nicht proaktiv? Unternehmen mit geringen Ressourcen benötigen darüber hinaus konkrete Unterstützung bei der NIS2-Umsetzung. Der Bundesrat hat dies bereits in Form von ausreichenden Finanzierungsstrukturen für Krankenhäuser gefordert. Eine gezielte Aufstockung der Mittel für das BSI kann ebenfalls hilfreich sein. Wenn diese sinnvoll und an der richtigen Stelle eingesetzt werden, hilft dies den Unternehmen, die bei der Umsetzung auf die fachliche Unterstützung durch das BSI zurückgreifen wollen. Auch die Vorfallmeldungen treffen in dem Fall nicht mehr auf ein Vakuum.

Zweitens: Es gibt viele offene Fragen zu den Meldefristen nach § 32 BSI-Gesetzentwurf. Die Frist bis zur ersten Meldung wurde auf europäischer Ebene auf 24 Stunden festgelegt, was aus unserer Sicht zu wenig Zeit ist. Dies kann nun allerdings nicht mehr angepasst werden. Daher muss jetzt zumindest die Anwendung der Frist geklärt werden. Beginnt die Frist, sobald der Vorfall als signifikant eingestuft wurde oder ab dem Zeitpunkt, an dem das Unternehmen vom Vorfall erfährt? Und was passiert, wenn ein Vorfall am Wochenende erst montags analysiert werden kann? Manche Interpretationen dieser Fragen würde ein IT-Service rund um die Uhr erfordern. Das ist für viele Unternehmen im Scope der NIS-2-Richtlinie nicht umzusetzen.

Drittens: Die Harmonisierung mit dem KRITIS-Dachgesetz lässt weiterhin große Lücken und das, obwohl die Abgrenzung zwischen physischer und digitaler Sicherheit fließend ist. Die regulierten Unternehmen brauchen Kohärenz und Rechtssicherheit. Ein voll funktionsfähiges NIS-2-Gesetz braucht ein entsprechendes KRITIS-Dachgesetz. Die Zeit dafür drängt angesichts der auslaufenden Legislaturperiode.

Abschließend möchte ich betonen, dass alle genannten Punkte umso weniger auf Verständnis in der Wirtschaft stoßen, wenn durch Ausnahmen für Einrichtungen der Bundesverwaltung in § 29 BSI-Gesetzentwurf eine große Glaubwürdigkeitslücke geschaffen wird. Dies gilt auch für die Ausnahmen durch die Entscheidung des IT-Planungsrates für die Kommunen und Länder. Auch hier bitten wir unbedingt um Nachbesserungen. Vielen Dank für Ihre Aufmerksamkeit. Weitere Details können Sie der schriftlichen Stellungnahme des Bitkom entnehmen.

AmtVors. **Petra Pau** (Die Linke): Herzlichen Dank. Das Wort geht an Frau Plattner.

SVe **Claudia Plattner** (BSI)**:** Guten Morgen und vielen herzlichen Dank für die Einladung und die Möglichkeit, zu diesem wichtigen Gesetz eine Stellungnahme abgeben zu dürfen.

Die Bedrohungslage ist im Cyberraum anhaltend hoch. Wir berichten kontinuierlich darüber, über die Einzelheiten, auch hier im Ausschuss. Insbesondere haben wir ein sehr hohes Risiko für kritische Infrastrukturen, Bundesverwaltung und politische Institutionen. Cybersicherheit ist inzwischen nationale Sicherheit, und die braucht dieses Gesetz dringend. Deshalb ist aus meiner Sicht die oberste Priorität, dass ein Gesetz zur NIS-2-Umsetzung schnell verabschiedet wird, damit wir in die Umsetzung kommen. Trotzdem sehe ich noch Nachbesserungsbedarf, den ich in einigen Punkten gerne aufzeigen möchte.

Bezüglich des Geltungsbereiches: IT-Sicherheitsvorgaben müssen für die gesamte Bundesverwaltung gleichermaßen gelten. Die aktuell formulierten Ausnahmen können wir uns nicht leisten, denn wir sind hier verwundbar. Ich verstehe, wie schwierig es war, auch nur diesen Kompromiss zu finden, aber wir haben auch ein massives Glaubwürdigkeitsproblem, wenn wir selber nicht bereit sind zu tun, was wir von der Wirtschaft erwarten.

Bezüglich des CISO: Die Bundesverwaltung braucht dringend Hilfe und Struktur bei der Bewältigung der Herausforderungen in der Cybersicherheit, auch in Form einer klaren CISO-Verantwortlichkeit. Das BSI hat hierzu bereits bestehende Organisationen geschaffen, die das am kompetentesten und aufwandsärmsten leisten könnten und das insbesondere neutral und ohne Bruch in der Zuständigkeit für den Prozess. Denn das BSI ist durch NIS-2 in jedem Fall zuständig. Deswegen möchte das BSI diese Aufgabe gerne auch richtig und ganz übernehmen. Wichtig sind die dazugehörigen Befugnisse im Gesetz zu verankern und keinen zahnlosen Papiertiger zu schaffen.

Zur Diskussion um ein unabhängigeres BSI, dessen Rolle gestärkt werden soll, wie im Koalitionsvertrag vereinbart, sind mir zwei Dinge wichtig:

Punkt Nummer eins: Wir werden auch weiterhin ein starkes Ministerium an unserer Seite brauchen. Das heißt, wir sehen keine Konstruktion wie zum Beispiel die der BfDI. Wir arbeiten gut mit den Kolleginnen und Kollegen des BMI zusammen. Unabhängigkeit muss aus meiner Sicht deshalb in der Wahrnehmung der fachlich-technischen Aufgabe festgeschrieben werden und durch eine Programmsteuerung statt Einzelerlasssteuerung auf ein strategisch stabiles Fundament gestellt werden.

Operative Abwehrfähigkeiten des BSI stärken: Hier geht es um Anordnungsbefugnisse des BSI gegenüber Domain-Anbietern. Ein sehr technisches Detail, aber eine Regelungslücke, die uns einfach Kraft nimmt und die Befugnis zur Messung der Resilienz der deutschen IT-Systeme gegenüber aktuellen Schwachstellen. Im Moment sind die Angreifer hier im Vorteil. Die suchen einfach nach Schwachstellen, um die Betroffenen anzugreifen, wohingegen wir nicht danach suchen dürfen, um die Betroffenen zu warnen. Das kann nicht sein.

Zu guter Letzt noch ein paar Worte zum Schwachstellenmanagement. Über einen Punkt sind sich alle Parteien einig. Schwachstellen, die das BSI in die Finger bekommt, werden in einem koordinierten Schwachstellenprozess der Schließung zugeführt. Das könnten wir schon mal ins Gesetz schreiben und damit „auf die Bank bringen“, wenn man so will. Andere Bereiche der Bundesregierung brauchen andere Regelungen. Das verstehe ich sehr gut. Und ein Weg nach vorne könnte hier sein, diesen nicht das BSI betreffenden Teil gegebenenfalls auszulagern und an anderer Stelle zu regeln.

Damit schließe ich mein Statement mit der erneuten Bitte einer zügigen Verabschiedung eines NIS-2-Umsetzungsgesetzes und freue mich auf Fragen.

AmtVors. **Petra Pau** (Die Linke): Vielen Dank. Das Wort hat Frau Prof. Schulmann.

SVe **Prof. Dr. Haya Schulmann** (Johann Wolfgang Goethe-Universität): Sehr geehrte Frau Vorsitzende, sehr geehrte Abgeordnete, meine Stellungnahme umfasst sechs Bereiche.

Erstens: Eine alle Verwaltungsebenen umfassende Umsetzung würde Synergien schaffen, Kosten senken und die Qualität der Cybersicherheit für alle verbessern. Leider vergeuden wir diese Chance, der Entwurf regelt nur die Bundesebene, nicht die genauso wichtige Landesebene. Selbst im Bund gibt es zahlreiche Ausnahmen. Alle Ausnahmen sollten auf das absolut Notwendigste reduziert werden.

Zweitens: Das BSI sollte wie vorgesehen im Geschäftsbereich des BMI bleiben, muss aber unabhängiger werden. Weniger Fachaufsicht durch das BMI, mehr Autonomie, unmoderierte Kommunikation und Vetorechte. Der CISO Bund sollte im BSI als faktische CISO-Organisation angesiedelt sein. Ein CISO neben dem BSI würde Redundanzen schaffen und die Autorität des BSI untergraben. Augenhöhe des CISO mit Bundesministerien lässt sich durch konkrete Festlegungen im Gesetz herstellen. Damit wir künftig auch politisch komplexe Themen einfacher angehen können, etwa die Einbeziehung der Länder, empfehle ich die Einrichtung eines unabhängigen Expertenrats für Cybersicherheit.

Drittens: Das BSI sollte die Länder und weitere Einrichtungen in Scans und Ähnliches einbeziehen dürfen. Nur so entsteht ein Gesamtbild, von dem alle und auch die Länder profitieren würden. Dazu gehört auch die Möglichkeit, die IT entlang der Lieferketten scannen zu dürfen, selbst wenn diese sich möglicherweise im Ausland befindet. Das BSI sollte nicht nur nach bekannten Schwachstellen, sondern auch nach Zero-Days suchen dürfen. Die derzeitige Einschränkung in §15 BSI-Gesetzentwurf ist irregeleitet. Statt die Suche zu untersagen, sollte das Gesetz festlegen, wie das BSI mit gefundenen Schwachstellen umgehen soll.

Viertens: Konkrete Verpflichtungen sind hilfreicher als vage Vorgaben. Es ist deshalb gut, den IT-Grundschutz für die Bundesregierung vorzuschreiben. Die sollte aber auf alle Verwaltungen ausgedehnt werden. Zudem deckt der IT-Grundschutz nicht alles ab. Vorgaben zur Umsetzung der Zero-Trust-Prinzipien wären deshalb sinnvoll, ähnlich wie dies 2022 in den USA gemacht wurde. Der Entwurf übersieht auch, dass DNS (Domaine Name System) nur eines von mehreren Kernsystemen des Internets ist. Genauso wichtig ist Routing-Sicherheit. Das White House hat dazu eine Roadmap für die USA veröffentlicht. Ich empfehle, Ähnliches auch bei uns zu tun.

Fünftens: Aktiver Cyberabwehr kommt im Entwurf kaum vor. Wir brauchen dringend einen umfassenderen Rechtsrahmen.

Sechstens: Wir können Sicherheit nicht ohne vertrauenswürdige IT erreichen. Der Entwurf belässt leider alles beim Alten. Das BSI kann nur eingeschränkt vor einzelnen Produkten warnen. Ich empfehle mehr Klarheit und Möglichkeiten vorzusehen.

Trotz aller Kritik möchte ich abschließend betonen, dass der Entwurf schon jetzt ein großer Schritt in die richtige Richtung ist. Es ist wichtig, dass wir die NIS-2-Richtlinie zügig umsetzen und dass das Gesetz einfach 2025 in Kraft treten kann. Vielen Dank für Ihre Aufmerksamkeit.

AmtVors. **Petra Pau** (Die Linke): Vielen Dank. Wir kommen nun in die Fragerunde. Ich erinnere nochmal an unsere Regeln. Sie benennen, ob Sie zwei Fragen an eine Sachverständige oder einen Sachverständigen stellen oder jeweils eine Frage an jeweils eine Sachverständige oder einen Sachverständigen. Dazu stehen zwei Minuten zur Verfügung und für die Antworten jeweils auch zwei Minuten. Das Wort hat der Kollege Hartmann.

Abg. **Sebastian Hartmann** (SPD): Sehr geehrte Frau Vizepräsidentin und amtierende Vorsitzende, herzlichen Dank. Wir freuen uns, dass wir diese Anhörung durchführen dürfen. Danke an die Sachverständigen. Um das Prozedere etwas zu ergänzen, würde ich mir die Fragen mit Herrn Kollegen Baldy aufteilen. Er würde die zweite Frage stellen.

Vielleicht sollten wir uns kurz nochmal erinnern. Wir sind froh, dass wir diesen Entwurf endlich beraten können. Der Koalitionspartner spricht von der Woche der Entscheidungen. Da stand man aber auch schon seit April letzten Jahres oft auf der Bremse, wenn da ganz viele Referentenentwürfe im Raum waren. Ich kann Ihnen versichern, wir hätten das gerne schneller gebracht. Deswegen danken wir Ihnen auch, dass der Entwurf jetzt da ist. Das KRITIS-Dachgesetz kommt jetzt auch endlich. Auch die Woche der Entscheidung an der Stelle, endlich sind die Blockaden auf Ebene der Bundesregierung gelöst. Das muss hier auch gesagt werden, denn das darf nicht nachher beim BMI hängen bleiben.

Frau Prof. Schulmann, ich möchte Sie gerne fragen. Sie haben etwas zu dem Thema Befugnisse des BSI ausgeführt, nämlich Warnung der Öffentlichkeit. Es geht darum, ein insgesamt höheres Niveau zu haben. Ich möchte jetzt nicht den föderalen Zusammenhang und das Zusammenspiel allein betrachten, sondern es geht auch um Unternehmen und Öffentlichkeit. Sie haben dazu rechtssichere Regelungen angemahnt. Können Sie das nochmal ausführen?
Ich würde gerne an Herrn Kollegen Baldy übergeben.

Abg. **Daniel Baldy** (SPD): Vielen Dank. Ich würde meine Frage auch an Sie, Frau Prof. Schulmann, richten. Das Thema Bundeseinrichtung: Sie haben auch in Ihrer Stellungnahme die Formulierung gewählt, dass die Ausnahmen auf das Mindeste verringert werden sollen. Geht es Ihnen da um eine qualitative Ausnahme oder eine qualitative Verringerung, also dass die Ausnahmen sich auf Maßnahmen beziehen? Oder geht es Ihnen um eine quantitative Ausnahme oder ein quantitatives

Minimum, dass quasi die Anzahl der Bundeseinrichtungen auf ein Minimum reduziert wird? Und wenn Sie da vielleicht nochmal konkreter sagen könnten, an welchen Stellen Sie Ausnahmen als sinnvoll erachten und an welchen, die der Gesetzentwurf aktuell formuliert, Sie die für nicht sinnvoll halten? Danke schön.

AmtVors. **Petra Pau** (Die Linke): Danke. Sie haben das Wort, Frau Professor.

SVe **Prof. Dr. Haya Schulmann** (Johann Wolfgang Goethe-Universität): Zur ersten Frage. Danke schön für die Frage. Im Jahr 2022 hat das BSI Warnung gegen Kaspersky ausgesprochen und es gab ganz viel Kritik gegen diese Warnung. Das zeigt, dass das Gesetz sich nicht klar zu diesem Thema äußert. Dieses muss geklärt werden. Warnungen sind sehr wichtig. Nicht nur vor einzelnen Produkten, sondern auch gegen die Hersteller, besonders jetzt angesichts der verschärften geopolitischen Lage. Wir sehen, dass es zunehmend Schwachstellen gibt, die absichtlich eingeführt werden. Zwar Schwachstellen in Betriebssystemen, Schwachstellen in anderen Produkten. In Bezug auf Kaspersky, ging es damals um Antivirus. Antivirus hat vollen Zugriff auf das System, auf dem es läuft, was natürlich erlaubt, alle Informationen abzugreifen und an Angreifer zu schicken oder an externe Angreifer, deshalb war die Warnung sicherlich sehr sinnvoll. Es ist wich-tig, dass das BSI diese Befugnis hat, und das muss im Gesetz auch gesichert werden.

Dann zur zweiten Frage. Die zweite Frage war, welche Einrichtungen sollten ausgenommen werden und welche nicht? Zum Beispiel die Wissenschaftseinrichtungen. Die Wissenschaftseinrichtungen spielen eine große Rolle für die Cyberangreifer. Es geht nicht nur darum, dass sie selbst angegriffen werden und Lösegeldforderungen und Verschlüsselung von Daten erhalten. So einen Fall gab es an der Universität Gießen und der TU Berlin. Die Angreifer hatten Zugriff zu Daten und haben Systeme verschlüsselt. Die Universität konnte nicht arbeiten, keine Gehälter zahlen und Studierende konnten nicht studieren. Das Schlimmste daran ist die hohe Reputation der Universitäten. Die Angreifer verwenden diese Systeme als Sprungbrett, um andere anzugreifen. Es erzeugt keinen Verdacht, da die Kommunikation aus IP-Adressen oder aus Rechnern kommt, die in Deutschland und an Universitäten sind. Dadurch können sie Angriffe durchführen, wie Spionage, Denial-of-Service-Angriffe oder andere Angriffe. Diese sind schwerer zu filtern oder zu blockieren, weil der Angriff aus Deutschland und nicht aus dem Ausland kommt. Das ist ein Beispiel für Einrichtungen, die stets angegriffen werden, um andere anzugreifen und spielen eine große Rolle für Deutschland und müssen geschützt werden.

Welche Einrichtungen sollten Ausnahmen sein? Das ist eine komplexe Frage. Die Ministerien, die ausgenommen werden, müssen sich selbst einschätzen. Das Auswärtige Amt zum Beispiel hat weltweit Ministerien. Dann könnte es strategisch-politisch schwerer sein, Scans oder Ähnliches oder NIS-2 in diese Ministerien umzusetzen. Man sollte jeden Fall getrennt betrachten und analysieren, um diese Frage beantworten zu können. Meine Empfehlung wäre, möglichst wenige Ausnahmen und möglich viele Einrichtungen dazu zu nehmen. Wenn wir erwarten, dass für kritische Infrastrukturen oder Unternehmen die Unterstützung und Umsetzung von NIS-2 verwendet werden soll, wieso sollte die Bundesregierung es selbst nicht tun?

AmtVors. **Petra Pau** (Die Linke): Herzlichen Dank. Kollege Henrichmann.

Abg. **Marc Henrichmann** (CDU/CSU): Auch von meiner Seite vielen Dank. Ich möchte die Forderung nach der Eingangsrunde vorwegschicken, dass dieser Streit in der Ampel endlich aufhören muss. Es geht um die Cyber-Sicherheit und ich glaube, wir sind uns an ganz vielen Stellen auch einig und nahe beieinander. Ich sehe auch gewisse Parallelen zur Anhörung rund um das Sicherheitspaket. Es wird aus der Riege der Sachverständigen beispielsweise ein Expertenrat gefordert. Es wird beklagt, dass mit der Wirtschaft, jedenfalls in der Anfangsphase, nicht hinreichend gesprochen worden ist. Das muss die Lehre sein, Druck auf den Kessel zu bringen, mehr als es bis dato der Fall ist.

Der CISO Bund ist auch ein Thema, wo wir schnell zueinanderkommen. Ehrlicherweise gibt es aber auch da leider traurige Parallelen zur Datenschutzkonferenz im Bundesdatenschutzgesetz. Sie haben wieder versäumt, inhaltlich oder strukturell zu beschreiben, auch mit Kompetenzen, was die Person tun soll. Bei der Thematik Zentralstelle kann man fordern, dass die Länder müssten, aber der Gesprächsfaden ist offenbar dauerhaft

blockiert. Den müssen Sie dringend wieder aufnehmen. Geld fürs BSI! Haushaltskürzungen, wie wir die jetzt gerade sehen, bringen uns nicht weiter. Und die Nicht-Erwähnung von Ländern und Kommunen, genauso wie die Herausnahme der nachgelagerten Bundesbehörden geht so nicht. Das KRITIS-Dachgesetz, das heißt nicht umsonst *Dach*gesetz, sondern es hat eine zentrale Funktion. Ich glaube, Herr Eisengräber hat es beschrieben, man kann manchmal den physischen Raum und den Cyber-Raum nicht klar trennen. Auch da haben wir im Juni einen Antrag formuliert, mit Erwartungen und Forderungen. Da haben Sie damals gelächelt und gesagt, das sei nicht genug. Die Kohärenz mit der KRITIS-Dachgesetz hätte mehr betont werden müssen. Wir stellen fest, wir sehen sie bis heute nicht. Außer der Ankündigung haben wir nicht viel gehört und deswegen eine Frage an Herrn Eisengräber und an Herrn Könen. Herr Eisengräber, Sie haben gesagt, die klare Abgrenzung der Räume sei nicht möglich. Jetzt aus Sicht der Wirtschaft, was sind Ihre Erwartungen an das KRITIS-Dachgesetz? Und auch der Kritikpunkt, was fehlt Ihnen, weil es noch nicht da ist? Herrn Könen, an Sie das Gleiche: Zum KRITIS-Dachgesetz würde mich Ihre Meinung nochmal vertieft interessieren. Danke schön!

AmtVors. **Petra Pau** (Die Linke): Dann beginnen wir mit Herrn Eisengräber.

SV **Boris Eisengräber** (Schwarz Digits)**:** Danke. Sie hatten auch schon die hybriden Angriffe erwähnt. Durchaus gibt es Angriffsszenarien, wo ein Angreifer sich zunächst physischen Zugriff zu Infrastruktur verschafft, um dann direkten Zugriff auf IT-Infrastruktur zu erlangen, um dann am Ende das Ziel zu erreichen, IT-Systeme zu kompromittieren. Insofern macht es keinen Sinn, Schutzkonzepte zu unterscheiden. Wir bei uns haben deswegen auch ein integriertes Schutzkonzept, was sowohl physische Angriffsszenarien als auch Angriffe auf IT gesamtheitlich betrachtet. Insofern macht es wenig Sinn, wenn wir an Registrierungs- und Meldepflichten denken, unterschiedliche Kategorien zu bilden und zu sagen, in einem Szenario ist eine Anlage, ein Unternehmen kritisch, in einem anderen Szenario nicht, weil nachher auch integrierte Angriffsszenarien denkbar sind. Insofern plädieren wir, wie Sie gesagt haben, dafür, im besonderen Melderegistrierungspflichten aufeinander abzustimmen und hier keine Unterscheidung zu treffen, die dazu führen, dass Physik und IT unterschiedlich behandelt werden.

AmtVors. **Petra Pau** (Die Linke): Danke schön. Herr Könen.

SV **Andreas Könen** (BIGS)**:** Den Aussagen von Herrn Eisengräber kann ich mich unmittelbar anschließen. Ich würde noch konkret mit Blick auf das KRITIS-Dachgesetz sehen wollen, dass das, was an Ansatzpunkten im NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz enthalten ist, sich dann auch eins zu eins im KRITIS-Dachgesetz wiederfindet. Das betrifft die Rollen von BBK und BSI. Beide sollten als Meldestelle fungieren und auch wechselseitig interagieren, sodass es nach außen damit einen Ansprechpartner für die Wirtschaft gibt. Ein sehr guter Ansatz, der im deutschen Umsetzungsgesetz enthalten ist, nämlich neben den wichtigen und besonders wichtigen Einrichtungen auch weiterhin Betreiber kritischer Anlagen mit zu implementieren, ist ein ganz wesentlicher Punkt, der sich jetzt auch im Analogen wiederum, das heißt erneut im KRITIS-Dachgesetz entsprechend wiederfinden muss, sodass die Vorschriften, die bereits heute teilweise im IT-Grundschutz auch die physische Welt betreffen, dann harmonisiert auf die Wirtschaft zukommen und damit zu einem einheitlichen Regelungsgefüge werden. Selten erwähnt wird dabei § 56 Absatz 4 BSI-Gesetzentwurf, die sogenannte KRITIS-Verordnung. Sie sollte entsprechend fortgeschrieben werden, sodass genau beide Seiten des Geschäfts auftauchen. Ein weiteres Anliegen ist eine Erweiterung des § 9b BSI-Gesetz, der jetzt als § 41 im Umsetzungsgesetz enthalten ist. Meiner Meinung nach gehört dieser Paragraf eigentlich ins KRITIS-Dachgesetz, denn es sind ja nicht nur Cybergefahren, die uns durch nicht vertrauenswürdige Hersteller aus dem Ausland begegnen, es sind genauso auch die Gefahren, die sich gegen die analogen Teile der Einrichtungen richten, wenn aus bestimmten Staaten Teile importiert werden und damit auch entsprechende Einflüsse entstehen. Danke.

AmtVors. **Petra Pau** (Die Linke): Vielen Dank. Wir machen weiter mit der Fraktionsrunde, Kollegin Khan.

Abg. **Misbah Khan** (BÜNDNIS 90/DIE GRÜNEN): Vielen Dank Frau Vorsitzende, vielen Dank an die Sachverständigen. Ich habe eine Frage an Frau Plattner und eine Frage an Herrn Kipker.

Zuerst die Frage an Frau Plattner: Was mich interessieren würde, Sie haben hier einmal ausgeführt, welchen Nachbesserungsbedarf Sie sehen. Können Sie noch mal konkreter auf die Punkte eingehen, die Sie angesprochen haben, bzw. auf weitere, die Sie vielleicht sehen, und welche Risiken für Sie darin bestehen, wenn da nicht nachgebessert wird?

Und an Sie, Herr Kipker, die Frage: Sie haben in Ihrer Stellungnahme von sehr vielen Schwächen und vielen Unklarheiten gesprochen, auch davon, dass es eine Zersplitterung gibt und auch unterschiedliche regulatorische Ebenen mit unterschiedlicher Verbindlichkeit, also eigentlich, dass wir von einer einheitlichen Umsetzung weit entfernt sind. Deshalb würde mich einmal interessieren, welche Möglichkeiten Sie sehen, hier noch mal zu einer besseren gesetzlichen Vorgabe zu kommen und auch zu einem kohärenten System, gerade auch, weil Sie richtigerweise sagen, dass wir in einer gestiegenen Bedrohungslage sind. Danke schön.

AmtVors. **Petra Pau** (Die Linke): Danke! Frau Plattner, Sie haben das Wort.

SVe **Claudia Plattner** (BSI): Danke schön. Ich würde gerne die Punkte noch einmal durchgehen und versuchen, ein kleines bisschen aufzuzeigen, was da die Gefahren und Risiken sind.

Bezüglich des Geltungsbereiches habe ich hier vor allen Dingen den Bund in Augenschein genommen, dort die Ausnahmen, über die wir gesprochen haben. Ich sehe hier einfach die Gefahr, dass wir verwundbare Einrichtungen des Bundes haben, die, wie Herr Könen auch schon richtig ausgeführt hat, gleichzeitig zusammen in den Netzen des Bundes zusammenarbeiten. Das heißt, wir haben hier einfach das Problem, dass wir dort Schwachstellen in der Gesamtarchitektur der Bundesverwaltung in Bezug auf Cybersicherheit einkaufen. Das halte ich für eine durchaus große Gefahr. Und ich hatte auch schon das Glaubwürdigkeitsproblem angesprochen. Die Wirtschaft erwartet natürlich, dass wir dasselbe leisten, was wir auch von Ihnen fordern. Das sind die beiden Punkte, die mich dort umtreiben, ich würde hier auch noch einmal das Bund-Länder Verhältnis ansprechen wollen. In der Tat, die Zentralstelle haben wir jetzt nicht mit aufgenommen in die Ausführungen. Nichtsdestotrotz ist das ein ganz, ganz wichtiger Punkt, wie wir zusammenarbeiten mit den Ländern und wie wir tatsächlich auch Informationen teilen. Das wäre ein weiterer Punkt, den ich noch anführen kann.

Bezüglich des CISO sehe ich die Gefahr, wenn wir es nicht schaffen, die Position mit entsprechenden Befugnissen auszustatten, dann haben wir eine Chance vertan, obwohl wir eigentlich die Bundesverwaltung dringend in ihrem Sicherheitsniveau anheben müssen. Wir brauchen dort eine klare Programmstruktur, ein klares Vorgehen. Mich erinnert das mehr an Projektmanagement als an Politik. Und ich glaube, auch genau das ist der Punkt, den wir hier brauchen. Das heißt, wir brauchen hier eine starke Ergebnisfokussierung und ein Anpacken dieser Themen auf einer technischen, organisatorischen Ebene, sehr unpolitisch, um dafür zu sorgen, dass wir hier wirklich die Meter machen. Deswegen sagen wir, wir als neutrale Stelle können das auch tun. Wenn wir das nicht mit entsprechenden Befugnissen ausstatten, wird das versanden. Das wäre außerordentlich schade. Nicht nur schade, sondern tatsächlich gefährlich, wenn ich das mal so sagen darf. Und ich sehe ein bisschen eine Gefahr, wenn wir das auf verschiedene Häuser aufteilen, sprich BSI und ein Ministerium, dass man dann, wie man das halt so kennt, wenn einem eine Vorgabe aus dem BSI nicht gefällt, erst noch mal woanders hingeht und noch mal guckt, ob nicht vielleicht dort noch mal eine andere Entscheidung kommt. Das halte ich für eine große Gefahr. Das wären die Punkte, die mir noch ganz wichtig sind. Danke.

AmtVors. **Petra Pau** (Die Linke): Das Wort hat Prof. Kipker.

SV **Prof. Dr. Dennis-Kenji Kipker** (Universität Bremen): Ich persönlich sehe drei ganz zentrale Aspekte, die meiner Meinung nach eine Rolle spielen. Einmal das Thema Vereinheitlichung des Cybersicherheitsniveaus in Bund und Ländern, das Thema Unabhängigkeitsstellung des BSI, das wurde auch schon mehrfach angesprochen, und eben das Thema klare Vorgaben und Unterstützungsleistungen für betroffene Wirtschaftsbetriebe. Wir berufen uns oft auf den Föderalismus, wenn wir sagen, das Cybersicherheitsniveau ist uneinheitlich. Aber Föderalismus bedeutet meiner Meinung nach auch irgendwo Selbstverwaltung in der Umsetzung. Also wir haben bereits ein Bund-

Länder-Gefälle in der Umsetzung von Cybersicherheit, und das nicht erst seit gestern, sondern bereits seit mehreren Jahren und das liegt einfach daran, weil wir mit dem Ersten IT-Sicherheitsgesetz angefangen haben, um zunächst eben die Privatwirtschaft zu regulieren. Dieses Defizit sollte nun eben mit dem NIS-2-Umsetzungsgesetz ausgeglichen werden. Wir müssen auch stärker diesen ganzheitlichen Ansatz betrachten. Das ist auch schon mehrfach angesprochen worden, also auch das KRITIS-Dachgesetz. Der Begriff ist jetzt bereits mehrfach gefallen. Das passt auch sehr gut, denn wir reden nicht mehr nur über Cybersicherheit, sondern heutzutage auch über digitale Resilienz. Das heißt, wir brauchen einen ganzheitlichen Ansatz und das ist auch das, was die geltende EU-Cybersicherheitsstrategie umsetzen will.

Was meiner Meinung nach noch zu weit ausgeklammert ist, ist die Umsetzung des Cyber Resilience Act, den wir seit diesem Herbst haben, der nicht diesen unternehmensbezogenen Schutz, sondern stärker den produktbezogenen Schutz in den Mittelpunkt stellt. Und das sollte meiner Meinung nach jetzt schon angestoßen werden, dass das auch vernünftig koordiniert wird. Diesen letztgenannten Punkt auch vertiefend: Es geht natürlich bei Cybersicherheit vor allem auch um Informationsaustausch. Beim BSI als Zentralstelle müssen die dafür erforderlichen Informationen zusammenlaufen. Und da kommen wir zur Debatte um die Unabhängigkeitsstellung des BSI. Cybersicherheit bedeutet Vertrauen. Und wenn Unternehmen sagen, dass sie Bedenken haben, dass sie teils hochsensible Daten oder Informationen abfließen lassen in Richtung des BSI und der Cybersicherheitsbehörden, weil sie nicht wissen, was damit geschieht, dann ist das ein großes Problem auch für die effektive Umsetzung von Cybersicherheit hier
in Deutschland. Und man braucht jetzt dieses Fass, glaube ich, nicht aufmachen. Über die Unabhängigkeit des BSI wurde schon viel diskutiert, aber es gibt durchaus verschiedene Möglichkeiten und Kompromisse, die allen Interessen gerecht werden können. Danke.

AmtVors. **Petra Pau** (Die Linke): Vielen Dank. Die nächsten Fragen stellt Herr Janich.

Abg. **Steffen Janich** (AfD): Vielen Dank. Meine zwei Fragen gehen an Frau Plattner. Die erste Frage: Der Kreis der Unternehmen wurde unter NIS-2 deutlich ausgeweitet. Was hier auf die betroffenen Unternehmen zukommt, ist in dem Sinne nicht unerheblich. Daher die Frage, welcher Erfüllungsaufwand kommt auf ein Unternehmen durchschnittlich zu, um den geänderten Sicherheitsvorgaben zu entsprechen?

Und meine zweite Frage wäre: Teilen Sie die Auffassung der Bundesregierung im Entwurf, dass die Umsetzung der Vorgaben zur Abwehr zur Hälfte des Schadens der angegriffenen Unternehmen führen wird, insbesondere unter der Maßgabe, wie das BSI derzeit personell ausgestattet ist und insbesondere darauf, welche Zusatzaufgaben dann noch auf das BSI zukommen? Vielen Dank.

AmtVors. **Petra Pau** (Die Linke):
Danke, Frau Plattner. Sie haben das Wort.

SVe **Claudia Plattner** (BSI)**:** Wunderbar. Sehr gerne. Danke schön.

Zunächst mal zum Erfüllungsaufwand. Wir sehen, dass in den Branchen, die bereits reguliert sind, also vor allen Dingen bei Banken, im Finanzbereich, aber auch im Bereich anderer kritischer Infrastrukturen, das Sicherheitsniveau dort deutlich nach oben gegangen ist. Wir haben jetzt keine direkte Pleitewelle erlebt aufgrund der Regulierungen. Also das ist leistbar. Wir empfehlen grundsätzlich zu sagen, dass man 20 Prozent seines IT-Budgets für die Sicherheit veranschlagen sollte – ob das von allen sofort erreicht werden kann, ist natürlich eine Frage. Ich glaube, das wird sich auch graduell steigern lassen. Ich glaube, dass jeder Invest in die Cybersicherheit im Moment ein Invest in das Risikomanagement einer Organisation ist, die sich am Ende des Tages massiv auszahlt. Dafür haben wir auch die Zahlen und die Belege. Denn einmal wirklich erwischt zu werden, und davor ist niemand gefreit, ist substantiell teurer. Das ist zunächst mal das, was ich dazu sagen kann: Es hängt von der Größe der Firmen ab, wie groß der Investitionsaufwand ist.

Wird NIS-2 zu einer Halbierung der Fälle führen? Ich hoffe, ich habe die Frage richtig verstanden. Ich würde es mir wünschen. Ich bin da auch sehr zuversichtlich. Für mich ist klar ist, dass die Umsetzungsfähigkeit nur in den Organisationen, in den Unternehmen und Institutionen selbst liegen kann. Die liegt nicht bei uns. Bei uns liegt die Supportfunktion und die Hilfestellung und die

Koordinierung dessen, dass wir das gut miteinander schaffen. Hierfür bin ich sehr zuversichtlich, dass, wenn Firmen das Thema Cybersicherheit klar auf die Agenda setzen, sie auch entsprechende Schutzwirkungen für sich selbst erzielen und wir auch einen deutlichen Rückgang der erfolgreichen Angriffe sehen werden. Ob es genau die Hälfte ist oder nicht, wage ich nicht zu prognostizieren. Ich erwarte mir viel von diesem Gesetz, das kann ich auch in aller Deutlichkeit sagen. Ich halte es für absolut notwendig, dass wir uns besser schützen. Das ist der Impuls, den die Organisationen brauchen. Wir selbst haben darin große Aufgaben und werden sie auch meistern müssen. Wir werden das mit den zur Verfügung stehenden Mitteln so gut wie möglich machen. Wir wünschen uns mehr. Wir würden gerne mehr und konkreter und weitergehend helfen. Wir werden das Beste aus dem rausholen, was wir dafür zur Verfügung haben, ob es reichen wird, werden wir sehen. Sie können sich darauf verlassen, wir werden unser Bestes geben.

AmtVors. **Petra Pau** (Die Linke): Vielen Dank. Das Fragerecht geht an den Kollegen Höferlin.

Abg. **Manuel Höferlin** (FDP): Vielen Dank, Frau Vorsitzende. Vielen Dank auch an Sie, liebe Sachverständigen, dass Sie so umfangreiche Statements geschickt haben und wir heute in das Gespräch kommen können.

Ich glaube, dass wir mit der Umsetzung der NIS-2-Richtlinie die Chance ergreifen sollten, all die Dinge, die die Cybersicherheit in Deutschland stärken können, auf den Weg zu bringen. Ich glaube, man sollte die Chance nutzen, viele Themen, die hier angesprochen wurden, mit abzuarbeiten. Das Schwachstellenmanagement ist gefallen, das BSI und die Strukturierung der Cybersicherheit in der Bundesregierung. Zu Recht wird auf den Föderalismus hingewiesen. Das ist aber eine Sache, die wir heute nicht abschließend lösen können, weil wir mit der Frage konfrontiert werden, wie wir Länder und Kommunen dazu bewegen können, bei den Dingen, die wir gemeinsam machen wollen, mitzugehen. Da gibt es einen großen Chor von Meinungen im Föderalismus und vor allem auch in der kommunalen Landschaft.

Ich würde mich gerne in der ersten Fragerunde auf den Themenkomplex Umsetzung und Meldesystem konzentrieren und Herrn Dr. Herpig die zwei Fragen stellen. Zum einen haben Sie selbst in Ihrer Stellungnahme die Herausforderungen für die Umsetzung und die Praktikabilität in Organisationen angesprochen. Sie haben auch von Bedenken zum Beispiel hinsichtlich der Belastung für kleine und mittelständische Unternehmen gesprochen, die Sicherheitsanforderungen umzusetzen. Deswegen wäre die erste Frage, welche konkreten Ideen Sie denn haben, wie man diese Herausforderungen umsetzbar machen kann, bei aller Notwendigkeit, die diese Unternehmen natürlich haben. Auch die Ausweitung auf den größeren Rahmen, gerade wenn man die Lieferkettenangriffe sieht, ist, glaube ich, gerechtfertigt. Aber es muss auch umsetzbar sein, weil es nichts hilft, etwas zu etablieren, was nachher nicht umgesetzt werden kann.

Das zweite ist das Meldesystem. Da ist hier auch schon Kritik angeklungen. Wie bewerten Sie denn dieses dreistufige Meldesystem und gibt es bei dem Meldesystem aus Ihrer Sicht Dinge, die man ändern kann, damit das effektiv bleibt und nicht nachher in quasi Nullmeldungen endet?

AmtVors. **Petra Pau** (Die Linke): Sie haben das Wort für beide Antworten.

SV **Dr. Sven Herpig** (interface): Wunderbar, vielen Dank. Was die Herausforderungen der Umsetzung angeht: Wer soll das denn alles umsetzen? Es sollen Menschen umsetzen, die IT-Sicherheit machen, die Firewalls konfigurieren, die Systeme aufsetzen und so weiter. Davon haben wir einfach schlichtweg jetzt schon nicht genug. Der 2024er ISACA State of Cyber Security Report besagt, dass 50 Prozent der deutschen und europäischen Unternehmen jetzt schon nicht ausreichend Fachkräfte finden und für die IT-Sicherheit haben. Wenn wir jetzt in Deutschland nochmal 30 000 bis 35 000 neue Unternehmen zu weiteren Vorgaben verpflichten, dann ist das für die IT-Sicherheit gut, aber erst dann, wenn wir jemanden haben, der es umsetzen kann. Das heißt, der Staat ist hier in der Pflicht, wenn er das umgesetzt haben will, das Ökosystem so zu gestalten. Das bedeutet, dass wir Aus- und Weiterbildungsmaßnahmen auf die Kette kriegen müssen, damit wir nicht in drei oder fünf Jahren zehn neue Master-Absolventen haben, sondern in sechs Monaten oder zwölf Monaten 5 000 neue Fachkräfte haben, die IT-Sicherheit machen können. Die müssen keinen kryptografischen Algorithmus schreiben können, die müssen

Firewalls konfigurieren können und so weiter. Wenn wir die nicht haben, dann krankt daran die ganze Umsetzung.

Damit gehe ich auch in die zweite Frage rein. Gleichzeitig dürfen wir, wenn wir uns bewusst sind, dass wir nicht genug Fachkräfte haben, die die Basics machen können und sollen, die Unternehmen nicht mit sinnlosen Maßnahmen überfordern. Anzuführen wäre hier u. a. dieser Paragraf zu den Schulungen. Wenn wir nicht nachvollziehen können, ob die Schulungen erfolgreich waren oder nicht, dann sehe ich jetzt ein paar Unternehmen, die sich freuen, dass sie leere Zertifikate ausstellen können an die ganzen Unternehmer, damit sie ihre Schulungen abgehakt haben. Das kostet Geld und Zeit, aber so richtig IT-Sicherheit haben wir davon nicht.

Der zweite Punkt, auch mit dem Meldesystem einhergehend: Ich soll Beinahe-Vorfälle melden. Nach der Definition, wissen Sie, wie viele Tausende Fälle jedes Unternehmen melden müsste? Das erinnert mich an die chinesische Gesetzgebung von vor ein paar Jahren, wo Unternehmen anzeigen sollten, wenn sie einen Datentransfer ins Ausland tätigen. Sie lächeln schon. Nach der Gesetzgebung ist eine E-Mail ein Datentransfer ins Ausland. Die Behörde wurde überflutet mit Meldungen und musste das Gesetz ändern. Bei Beinahe-Vorfällen sehe ich das ähnlich. Wir machen den kompletten Vorteil der Meldungen kaputt, wenn da jeder jeden Beinahe-Vorfall melden soll. Gleichzeitig belasten wir die Unternehmen, die eh schon keine Fachkräfte haben. Ich sehe da überhaupt keinen Mehrwert. Und einen Rückkanal wird es auch nicht geben, das heißt, ich melde da irgendwie hunderte Beinahe-Vorfälle und dann kriege ich auch keine Rückmeldung vom BSI, wobei das BSI dann natürlich auch überfordert ist. Das halte ich für sehr sinnbefreit.

AmtVors. **Petra Pau** (Die Linke): Danke schön. Dann sind wir in der ersten Runde rum. Kollege Hartmann oder Kollege Baldy? Kollege Baldy.

Abg. **Daniel Baldy** (SPD): Danke schön. Meine Frage oder zwei Fragen richten sich an Herrn Kuhlenkamp.

Die erste Frage dreht sich auch um das Thema Meldewesen. Es gab insbesondere zu den Referentenentwürfen immer auch die Bitte, dass es ein einfaches Meldewesen gibt. Ich habe aus den bisherigen Äußerungen gehört, dass zumindest die meisten oder alle dieses Meldewesen oder die gemeinsame Meldestelle von BSI und BBK gutheißen. Sehen Sie darüber hinaus, insbesondere aus den Änderungen, die sich nicht aus dem BSI-Gesetz, sondern beispielsweise dem Telekommunikationsgesetz hinsichtlich Meldewegen noch ergeben, noch Änderungshandlungsbedarf?

Die zweite Frage wäre etwas, das auch von Ihnen angesprochen wurde, nämlich das Thema Einsatz kritischer Komponenten. Sie haben es in Ihrer Stellungnahme zumindest grundsätzlich so geschrieben, so habe ich es vernommen oder gelesen, dass die Versagung des Einsatzes ermöglicht wird, dass das gut geheißen wird und gleichzeitig auch darum gebeten, dass man es einfacher macht. Wenn Sie da vielleicht kurz skizzieren könnten, wie diese Versagung des Einsatzes kritischer Komponenten in Ihren Augen oder Ihres Verbandes einfacher gestaltet werden könnte?

AmtVors. **Petra Pau** (Die Linke): Danke, Sie haben das Wort zur Beantwortung.

SV **Felix Kuhlenkamp** (Bitkom)**:** Vielen Dank für die Fragen. Um auf die erste Frage in Richtung Meldewesen einzugehen. Grundsätzlich ist hier der Bürokratieaufwand möglichst gering zu halten. Das ist aus den Stellungnahmen der anderen Experten und Expertinnen hervorgegangen. Was wichtig ist, ist zu betonen, das gilt für alle Sektoren, ob es Telekommunikation, kritische Infrastruktur, Banken oder Ähnliches ist. Es ist wichtig, in einem Krisenfall schnell reagieren zu können. Das bedeutet, man sollte die Ressourcen, die einem zur Verfügung stehen im Krisenfall, nicht darauf verwenden, sich zu überlegen, zu welcher Behörde ich mich jetzt wenden muss. Muss ich mich mehrfach bei Behörden melden? In dem Fall sollte es wichtig sein, eine zentrale Anlaufstelle zu haben, bei der klar ist, wir melden das jetzt. Es ist wichtig, dass es gemeldet wird. Um sich auch dann der Aufgabe der Bewältigung widmen und sie angehen zu können. BBK, BSI, wie gesagt, wir sind gespannt, was jetzt mit dem KRITIS-Dachgesetz passiert, wenn das harmonisiert ist. Wir sind wir auf einem guten Weg. Das gleiche gilt auch für die anderen Industrien und Branchen. Wenn wir zum Einsatz von kritischen Technologien und Ähnlichem gucken, dann gilt auch hier derselbe Punkt. Wir setzen uns in der Stellungnahme dafür

ein, dass auch das weiterhin nach technologischen Maßnahmen erfolgen soll, da vertrauen wir auch wie bisher auf die Einschätzung des BSI und auch hier sei nochmal die Bürokratiearmut zu betonen, dass das besonders wichtig ist, dass die Unternehmen Klarheit haben, an wen müssen sie sich wenden können, wo die Anforderungen herkommen, und was sie erfüllen müssen.

AmtVors. **Petra Pau** (Die Linke): Vielen Dank. Kollege Henrichmann.

Abg. **Marc Henrichmann** (CDU/CSU): Vielen Dank. Ich würde gerne in der zweiten Runde zwei Fragen an Prof. Kob stellen.

Einmal zum § 29 BSI-Gesetzentwurf: Wir haben gerade schon über die Länder und Kommunen gesprochen und den Aberwitz, beispielsweise Baugenehmigungsbehörden und Co., die dann Pläne haben, auszunehmen, wenn nebenan der gut geschützte KRITIS-Betreiber über den Weg angegriffen wird. Das ist eine offene Flanke. Aber das Thema Ausnahmen für die nachgelagerten Bundesbehörden würde ich gerne aufmachen. Sie sprechen vom § 29 im BSI-Gesetzentwurf als Horrorkabinett für alle sicherheitsaffin denkenden Personen. In der Tat sind die Bundesbehörden ausgenommen von Risikomanagementmaßnahmen, Überwachungs- und Schulungspflichten für Amtsleitungen und Kursen. Aufsichts- und Durchsetzungsmaßnahmen durch das BSI sind eigentlich untergraben oder gar nicht existent. Was konkret sind da Ihre Szenarien? Warum appellieren Sie so eindringend dafür, die nachgelagerten Bundesbehörden aufzunehmen?

Und der zweite Punkt: Sie haben in Ihrer Stellungnahme sehr dezidiert den Ablauf beschrieben, wie nach und nach diese Aufweichung vonstattenging. Und am Ende blieb jetzt eine dreijährige Karenzzeit für KRITIS-Betreiber über. Das heißt, wenn man so will, soll Kontrolle erst mal gar nicht erfolgen können. Es schwebt das Thema Managerhaftung immer noch im Raum, aber auch der Einfluss auf die Cybersicherheit insgesamt. Wie bewerten Sie den? Zur Karenzzeit stellt sich auch die Frage von Versicherungspolicen oder auch Gerichtsentscheidungen. Das heißt, wir haben eine dreijährige Übergangsphase, wo eigentlich Europarecht gilt und umgesetzt sein müsste. Was sind da konkret Ihre Befürchtungen für KRITIS-Betreiber hier in Deutschland, wenn man diesen Gesetzentwurf jetzt so umsetzen würde, wie er formuliert ist?

AmtVors. **Petra Pau** (Die Linke): Vielen Dank, Sie haben das Wort zur Beantwortung.

SV **Prof. Timo Kob** (HiSolutions)**:** Vielen Dank für die Fragen. Das gibt mir gleich noch die Möglichkeit, auf einen Fehler meiner eigenen Stellungnahme einzugehen. Die Schulungen werden im ersten Schritt rausgenommen und fünf Paragrafen später wieder reingenommen. Amtsleiter müssen sich schulen lassen. Das ist mein Fehler gewesen, dass ich nur das Explizite rausnehme und nicht das Implizierte reinnehme. Bisher wäre, wir können drei Plätze nach links schauen, ist das BSI verpflichtet, die eigenen Standards einzuhalten durch den Umsetzungsplan Bund. Sie müssen IT-Grundschutz umsetzen. Das klingt auch logisch, wenn man sich selbst etwas ausdenkt, dass man es auch selbst umsetzen muss. Dies ist in Zukunft nicht mehr der Fall, weil genau diese ganzen nachgelagerten Gewohnheiten ausgenommen worden sind. Das ist der Grund, weshalb ich von einer Schwächung gesprochen habe, weil wir hier sogar auf einen Stand zurückgehen, den wir schon einmal hatten. Dafür ist keine sinnhafte Begründung zu finden. Bei dem ganzen Thema Ausnahmen, Frau Schulmann hatte das Thema auch schon, wer soll denn ausgenommen werden? Ja, genau, so wenig wie möglich und dann auch nicht in der Gänze. Ein Beispiel, Auswärtiges Amt. Ich verstehe ja, dass bestimmte Teile, die im Ausland betrieben sind, dass da der IT-Grundschutz vielleicht nicht passt, weil ich bestimmte Punkte nicht habe. Aber dann kann man vielleicht einen umgekehrten Weg wählen. Es ist erst mal alles drin, um im Einzelfall nachzuschauen, wie ich diese Einzelfälle anders regeln kann. So werden große Lücken geschaffen, die nicht vorhanden sind und für die es keinen Grund gibt. Es geht bis in die einzelnen Ebenen runter. IT- Dienstleister für Länder und Kommunen, die wollen reguliert werden. Den schlimmsten Fall, den wir in Südwestfalen hatten, da haben die ein Jahr gekämpft. Die bitten darum, reguliert zu werden, werden es aber nicht. Das ist das zweite Thema, was dahintersteht, wo es einfach keine vernünftigen Gründe gibt. Ja, es ist schwierig, es umzusetzen, aber es ist ein dickes Brett, nicht ganz so dick wie das Brett Föderalismus, aber immer noch dick genug. Deswegen zu sagen, ich stecke den Kopf in den Sand, ist nicht die richtige Antwort.

Die zweite Frage war das Thema Karenzzeit. Aus meiner Sicht ist das ein Fehler, der in Brüssel passiert ist. Niemand hat darüber nachgedacht, dass man es irgendwann mal umsetzen muss und das von dem Moment, ab dem es das Gesetz gegeben hat und es in Kraft getreten ist. Jetzt kann man sagen, wir reden schon drei Jahre über NIS-2, hätten ja alle machen können. Wenn man aber noch nicht genau weiß, wer davon betroffen ist, hätte ich mir gewünscht, dass alle schon beginnen, weil es auch für die, die nicht NIS-2-relevant sind, sinnvoll ist. Aber so ist die Welt nicht. Wir werden in eine Phase laufen, wo das Gesetz gilt, viele feststellen, dass sie es umsetzen müssen und erst dann an den Punkt kommen. Dann war der Schritt, wir finden einen Weg, dass wir sagen, wir prüfen es nicht gleich, ihr habt erst mal Zeit, diese drei Jahre „Karenzzeit“, wie ich es genannt habe, bis wir den Nachweis erbringen müssen. Übrigens hätte ich mir sogar gewünscht, dass mehr nachweisen müssen, jetzt sind ja viele, die gar nicht nachweisen müssen, da hätte man vielleicht mehr machen können. Das Problem ist nur, nicht nachweisen, gegenüber, es passiert etwas, das sind ja zwei verschiedene Dinge. Was ist, wenn in zwölf Monaten jemand Opfer eines Ransomware-Vorfalls wird und dann vor Gericht oder bei der Cyberversicherung gesagt wird, aber du bist doch seit einem Jahr gesetzlich dazu verpflichtet, dies zu machen, du musst es nur nicht nachweisen? Damit entfällt doch gegebenenfalls der Schutz durch die Versicherung, damit werde ich schadensersatzpflichtig gegenüber Leuten, die dadurch einen wirklichen Schaden erlitten haben. Das heißt, wir suggerieren den Unternehmen, ihr habt drei Jahre Zeit, aber eigentlich haben sie nicht einen Tag Zeit. Und nicht ein Tag Zeit zu haben, ist da vollkommen weltfremd. Hier haben wir einfach eine Regelungslücke, wo eine große Ratlosigkeit in der Wirtschaft entsteht.

AmtVors. **Petra Pau** (Die Linke): Vielen Dank. Kollegin Khan.

Abg. **Misbah Khan** (BÜNDNIS 90/DIE GRÜNEN): Vielen Dank. Die Fragen gehen an Herrn Kipker. Thema unklare Rollen der einzelnen Aufsichtsbehörden, war bei Ihnen ein Thema, ist bei uns ein Thema. Wir wissen seit langem, gerade mit Blick auf die Absenkung der Schwellenwerte, dass mehrere zehntausende private Anbieter, darunter auch viele KMUs (Kleine und mittlere Unternehmen), vor besonderen Herausforderungen stehen, weil sie sich zum Teil noch nicht damit befasst haben, wir uns damit noch nicht ordentlich befasst haben. Das heißt, es droht eine enorme Herausforderung durch die Kohärenz, die noch nicht gegeben ist und es bedarf einer guten Abstimmung, die notwendig ist, zwischen den verschiedenen Behörden und den unabhängigen Beratungen.

Deshalb ist meine Frage, droht nicht vielleicht auch ein Durcheinander von verschiedenen Aufsichtsbehörden mit den Anbietern, gerade mit Blick auf die unterschiedlichen Vorgaben, die es gibt in Bezug auf Schutz physischer und digitaler Infrastrukturen und stehen eigentlich auch genug Kapazitäten für die Aufsichtsbehörden zur Verfügung, für eine gute unabhängige Beratung? Was halten Sie in dem Kontext von der Idee des sogenannten One-Stop-Shops? Ist hier auch schon angesprochen worden. Das heißt, dass Anbieter eine Stelle haben, an die sie sich wenden können und dass sich die Aufsichtsbehörden darum kümmern müssen, dass das gut koordiniert ist.

Die zweite Frage ist gerichtet auf den Bezug auf Datenschutz, den Sie in Ihrer Stellungnahme ja auch angesprochen haben. Sie haben jetzt hier auch schon von der teils sogar unionsrechtswidrigen Situation gesprochen. Was mich interessieren würde, ist, weil die BfD selbst ja heute nicht da ist, ob aus Ihrer Sicht die BfD ausreichend eingebunden und in der Gesetzgebung berücksichtigt ist. Danke.

AmtVors. **Petra Pau** (Die Linke):
Vielen Dank. Sie haben das Wort.

SV **Prof. Dr. Dennis-Kenji Kipker** (Universität Bremen): Vielen Dank für die Fragen. Man muss vielleicht dazu vorwegsagen, im europaweiten Vergleich ist die Zersplitterung der Aufsicht über die Einhaltung von gesetzlichen Vorgaben zur Cybersicherheit keine Ausnahme. Wir sehen in verschiedenen mitgliedstaatlichen Einrichtungen auch, dass Doppelzuständigkeiten bestehen und teilweise keine zentralisierte Befugnis vorhanden ist. Von daher sind wir in Deutschland schon einen Schritt weiter, weil wir eben eine zentrale Cybersicherheitsbehörde haben. Nichtsdestotrotz ist es so, dass wir auch in Deutschland beachten müssen, dass wir keine Durchmischung von Zentralisierung mit dem BSI einerseits und einzelnen Fachbehörden andererseits haben. Wir haben beispielsweise auch die BaFin oder die

Bundesnetzagentur, die für den Bereich Cybersicherheit ebenfalls Zuständigkeiten besitzen. Mit dem KRITIS-Dachgesetz und diesem holistischen Ansatz in Einbeziehung natürlich des BBK, wird sich das für diesen speziellen Ansatz der Regulierung wahrscheinlich noch weiter deutlich verschärfen. Wenn wir uns den gegenwärtigen Entwurf anschauen, dann kann man, glaube ich, ganz gut schon erkennen, dass die Bestrebungen da sind, Dinge, Verwaltungsverfahren, dort auch zu erleichtern. Für mich ist das beste Beispiel, dass die Meldung durch eine Meldestelle zentralisiert wird, aber das ist noch nicht an der Stelle zu Ende gedacht. Wir haben eine ganze Anzahl an datenrelevanten Vorfällen, die gemeldet werden können. Das hatte ich im Rahmen meiner Stellungnahme schon angemerkt. Für die Unternehmen ist es eben nicht immer klar, an wen ich mich jetzt eigentlich wenden soll, ob es jetzt ein physischer Vorfall ist oder ein rein physischer Vorfall, der auch mit IT zusammenhängen kann, ob es ein reiner IT-Vorfall ist. Diese Unterscheidung, die kann den Unternehmen an der Stelle nur ganz schwer zugemutet werden. Wir müssen eben aufpassen, dass wir, wenn wir in die Umsetzung von NIS-2 kommen, nicht zu einem Punkt kommen, wo die Meldung von sicherheitsrelevanten Informationen unterlassen wird, weil sich Unternehmen unsicher sind, also rechtsunsicher sind, oder vielleicht eine Sorge vor Haftung sogar oder vor Bußgeldern haben.

Der zweite Teil dieser ersten Frage bezog sich auf die Kapazitäten. Ich glaube, da kann man ganz aktuell sagen, dass diese nicht ausreichend sind. Vor allem sehe ich mit Besorgnis, dass teilweise auch einzelne Bundesländer – und das sind nicht in erster Linie Flächenstaaten – sich eben teilweise auch darauf verlassen, politisch und natürlich auch fachlich, dass das BSI an der Stelle schon irgendwie richten wird. Das ist gefährlich. Wenn eine Behörde deshalb, vielleicht den letzten Teil dieser Frage adressierend, mit ausreichenden Kapazitäten ausgestattet ist und auch hinreichend unabhängig ist, dann halte ich diese Lösung eines One-Stop-Shops sicherlich für sinnvoll. Cybersicherheitsmanagement ist erst einmal eine rein betriebsinterne Aufgabe, das hat Claudia Plattner auch richtigerweise gesagt, und die Unternehmen sind gefordert, das Ganze umzusetzen. Aber alles, was irgendwie mit Verwaltung, mit Behördenkommunikation zu tun hat, das kommt eben on top. Diese Mehrbelastung sollte eben so gering wie möglich gehalten werden. Da hilft so ein One-Stop-Shop durchaus.

Die zweite Frage nochmal kurz adressiert. Ich hatte das mehrfach in meiner Stellungnahme angemerkt. Das Thema Datenschutz halte ich nicht für ausreichend berücksichtigt, weil eben die meisten Cybersicherheitsvorfälle auch automatisch irgendwo Datenschutzvorfälle sind. Wir sehen das allenthalben, ob es jetzt im KRITIS-Sektor Gesundheit ist, wo eben zigtausend Datensätze mal eben so abhandenkommen. Das endet dort nicht. Bei den durch die NIS-2-Richtlinie kernbetroffenen Wirtschaftsbetrieben spielt das eine Rolle, wo wir eben Unternehmen haben, wo nicht nur Geschäftsgeheimnisse abhandenkommen, also Blaupausen, Sourcecode, Maschinenbauunterlagen, sondern wo eben auch Personaldaten, hochsensible Daten abhandenkommen. Wir müssen das Ganze auch unter diesem Gesichtspunkt ganzheitlich denken. IT-Systeme verarbeiten nicht nur nicht-personenbezogene Daten, sondern auch personenbezogene Daten, was auch sehr gut daran erkennbar ist, dass eben diese klassische Trennung zwischen IT- und OT-Security (OT: Betriebstechnologie) immer weiter verschwimmt und man das auch nicht aufrechterhalten kann. Cybersicherheit bedeutet irgendwo auch Vertrauen. Auch das Vertrauen darin, dass mit diesen ganzen verarbeiteten Daten auch im behördlichen Kontext vertrauensvoll umgegangen wird. Ich sehe da derzeit noch deutlich Luft nach oben. Wir haben jetzt eine Stellungnahme von der BfDI erhalten, die heute eingereicht worden ist. Die konnte man jetzt noch nicht im Einzelnen inhaltlich überprüfen. Das ist aber durchaus ein Schritt in die richtige Richtung. Ich würde mir wünschen, dass solche Dinge dann auch vorher im Gesetzgebungsverfahren adressiert werden, sodass der Datenschutz und dieses Zusammenwirken von Datenschutz, da meine ich einerseits Datenschutzverletzung, aber auch präventiven technischen Datenschutz und Cyber-Sicherheit, – –

AmtVors. **Petra Pau** (Die Linke): Achten Sie bitte auf die Zeit.

SV **Prof. Dr. Dennis-Kenji Kipker** (Universität Bremen): – – dass die noch deutlicher zusammenfinden. Danke.

AmtVors. **Petra Pau** (Die Linke): Danke. Bevor wir weitermachen: Es lag und liegt in der Hand der

Fraktionen, ob die Beauftragte für den Datenschutz und die Informationsfreiheit angehört wird. Insofern müssen das die Fraktionen im Vorfeld einer solchen Anhörung miteinander klären, weil das jetzt hier mehrfach aufgerufen wurde, auch durch Kollegen. Gut, wir machen weiter. Herr Janich, Sie haben das Wort.

Abg. **Steffen Janich** (AfD): Vielen Dank. Meine erste Frage geht an Herrn Kuhlenkamp und meine zweite Frage geht an Herrn Dr. Herpig.

Die erste Frage, finden Sie die Dreiteilung der Meldepflicht für sicherheitsrelevante Vorfälle nach einem Tag, nach mehreren Tagen, nach einem Monat gelungen und sinnvoll?

Und meine zweite Frage an Herrn Dr. Herpig. Wie viele Unternehmen in Deutschland sind aus Ihrer Sicht von der gesetzlichen Änderung betroffen und wie lange wird die Umsetzung der Vorgaben des neuen BSI-Gesetzes für die mittelständischen Unternehmen aus Ihrer Sicht in der Praxis dauern? Vielen Dank.

SV **Felix Kuhlenkamp** (Bitkom)**:** Zur Frage nach den Meldefristen. Wie gesagt, in meiner Anfangsstellungnahme habe ich bereits erwähnt, dass wir davon überzeugt sind, dass die 24 Stunden für die erste Meldung zu kurz sind. Wir sind schon davon überzeugt, dass es Sinn macht, das zu staffeln. Wir sind allerdings jetzt auch an einem Zeitpunkt, wo sich das nicht mehr ändern lässt. Das ist eben auf europäischer Ebene passiert. Da kann man im Nachhinein keine Vorwürfe mehr machen oder groß darüber streiten. Ich glaube, es ist eine Frage, die Definition zu klären und klarzumachen, dass insbesondere Unternehmen, die kleine und mittlere Unternehmen sind, und eben nicht einen Rund-um-die-Uhr-IT-Service zur Verfügung stellen können, jetzt vielleicht nicht ab Sonntag, 14.00 Uhr die 24 Stunden Zeit haben sollten, das zu melden. Ideal wäre der Zeitpunkt, wenn sie davon Erkenntnis bekommen, dass es ein erheblicher Sicherheitsvorfall ist.

AmtVors. **Petra Pau** (Die Linke): Danke schön. Kollege Höferlin. Entschuldigung, wir hatten ja noch die zweite Frage. Entschuldigung.

SV **Dr. Sven Herpig** (interface): Wie viele Unternehmen betroffen sind? Ich kann es nicht nachvollziehen, ich kann es nicht nachrechnen. Die Zahlen, die im Raum schweben, sind um die 30 000, glaube ich. Das nehme ich jetzt erstmal so hin. Was die Umsetzung angeht, das ist natürlich sehr heterogen. Sie haben sehr heterogene IT-Infrastrukturen in den KMUs. Sie haben einen absolut heterogenen Zustand der IT-Sicherheit in den KMUs. Die Frage ist, wie viel Geld können und wollen Sie ausgeben, auch in Bezug auf Fachkräfteanwerbung? Kann ich überhaupt Fachkräfte anwerben? Wie lange wird es dauern, bis ich Fachkräfte finde, die ich anwerben kann? Werden mir die weggekauft? Wenn ich 30 000 Unternehmen über Nacht reguliere, dann werden die sich alle auf die Suche nach IT-Fachkräften machen, die wir, wie wir gerade besprochen haben, nicht oder nicht im ausreichenden Maße haben. Von daher ist es unmöglich, eine Aussage darüber zu treffen, wie lange diese Umsetzung der Maßnahmen für das einzelne KMU dauern wird. Ich gehe hier eher von Monaten und Jahren als von Tagen und Wochen aus.

AmtVors. **Petra Pau** (Die Linke): Vielen Dank. Nun hat der Kollege Höferlin das Wort.

Abg. **Manuel Höferlin** (FDP): Vielen Dank, Frau Vorsitzende. Ich habe eine Frage an je einen Sachverständigen. Zuerst an Herrn Eisengräber. Mich würde aus Ihrer Sicht das Thema Meldungen von Vorfällen und das bereits angesprochene Thema Rückkanal von Meldungen interessieren. Ich habe in der Vergangenheit auch immer bei den IT-Sicherheitsgesetzen 1.0 und 2.0 kritisiert, dass sie immer Einwegkommunikation hatten. Das wurde leider damals nie ernst genommen, sondern es war im Prinzip immer eine Einbahnstraße. Das habe ich mir vorgenommen, in Zukunft anders zu gestalten. Von daher bin ich an einem Blick aus der Praxis sehr interessiert. Sie sind ein Unternehmen mit unterschiedlichen breiten Strukturen. Das heißt, Sie melden ja auch innerhalb Ihres Unternehmens wahrscheinlich Sicherheitsvorfälle unterschiedlicher Personen. Meine Frage ist, wie stellen Sie sich das vor, wie können Sie in Ihrem Unternehmen Meldungen am besten organisieren und was erwarten Sie als Rückkanal, damit Sie nicht irgendetwas zurückgemeldet bekommen, sondern etwas, mit dem Sie etwas anfangen können für Ihre Sicherheit?

Die zweite Frage geht an Herrn Dr. Herpig. Sie haben in Ihrer Stellungnahme zum Thema Schwachstellen ausgeführt, dass Sie sich auch eine

Meldepflicht für Unternehmen für Schwachstellen wünschen. Zumindest meine ich, dass so gelesen zu haben. Aber wir reden bisher über den Satz, der aus dem Koalitionsvertrag stammt, dass alle staatlichen Stellen ihnen bekannte Schwachstellen zu melden haben. Verbunden mit dem Punkt, wer sollte denn noch alles Schwachstellen an das BSI melden und unter welchen Organisationsregeln? Wie sollte ein ordentliches Schwachstellenmanagement aussehen und sollte es Ausnahmen davon geben und wenn ja, wie? Das würde mich interessieren.

AmtVors. **Petra Pau** (Die Linke): Danke. Herr Eisengräber.

SV **Boris Eisengräber** (Schwarz Digits): Trotz der Heterogenität unserer Geschäftsfelder haben wir eine zentrale Koordinationsstelle. Auch bei uns geht es um die Bündelung von Kompetenzen, die Sicherheitsvorfälle bearbeitet und koordiniert. Insofern ist das auch die Stelle, die dann die behördlichen Meldungen durchführen wird. Im konkreten Sicherheitsvorfall ist es aus unserer Sicht gar nicht so erheblich, dann direkt irgendwo Rückmeldung zu bekommen, denn diesen konkreten Vorfall müssen wir allein bewältigen. Das liegt in der Verantwortung der Unternehmen. Das, was wir uns aus den erweiterten Meldepflichten erhoffen, ist ein erweitertes und verbessertes Lagebild und auch rechtzeitige und schnelle Informationen auf Basis der Informationen, die andere Unternehmen uns bereitstellen. Das ist auch der Grund, warum wir sagen, der vorliegende Gesetzentwurf kann nur seine gewünschte Wirkung entfalten, wenn das BSI auch mit ausreichenden Ressourcen ausgestattet wird, um dann diese Meldungen zeitgerecht zu verarbeiten und dann der Wirtschaft auch wieder zurückzuspielen in detaillierteren Lagebildern, Warnungen und Empfehlungen. Das heißt aus meiner Sicht, nein, nicht konkret in einem bestimmten Sicherheitsvorfall, sondern eher in der Konsolidierung der Informationen und der Bereitstellung und dem Zurückspielen an die Wirtschaft.

SV **Dr. Sven Herpig** (interface): Ich würde für keine Meldepflicht für Unternehmen plädieren, sondern ich würde einfach positive Anreize schaffen, Rechtssicherheit für Sicherheitsforscher und so weiter, damit, wenn ich eine Schwachstelle finde, als Unternehmen oder als Sicherheitsforscher, die melden möchte. Ich würde keinen staatlichen Zwang daraus machen. Dazu muss ich Rechtssicherheit haben und auch den Prozess verstehen und wissen, was mit meiner Schwachstelle geschieht, wenn ich sie irgendwo hingebe.

Zum Thema, wie soll ein staatliches Schwachstellenmanagement aussehen: Wir haben 2018 ein Papier dazu veröffentlicht. Ich fasse es kurz zusammen. Ich sehe es zweigeteilt. Schwachstellen, die dem BSI mitgeteilt werden, damit die Schwachstelle geschlossen wird, die müssen, das hat Frau Plattner vorhin ausgeführt, dann auch durch das BSI direkt an den Hersteller/Produktverantwortlichen gemeldet werden, damit die geschlossen wird. Da gibt es nichts drumherum, da kann nichts anderes mit dieser Schwachstelle geschehen. Wenn ich als Sicherheitsforscher eine Schwachstelle beim BSI melde, muss ich darauf vertrauen können, dass das BSI das macht, zum Schutze der IT-Sicherheit, wofür es da ist. Von daher, die Paragrafenänderung, die vorhin von der Präsidentin genannt wurde, würde ich unterstützen. Gleichzeitig sollte es einen zweiten Teil geben, nämlich Schwachstellen, die zum Beispiel beim Bundesnachrichtendienst gefunden werden vom Bundeskriminalamt oder vielleicht von Sicherheitsforschern, die gerne den Bundesnachrichtendienst bei seiner Aufgabe unterstützen wollen und nicht das BSI bei seiner Rolle unterstützen wollen. Die müssten auch eine Möglichkeit haben, etwas in einen Prozess zu geben. In diesem Prozess wird die Schwachstelle angeschaut und wird geschaut, ob sie direkt gemeldet wurde, was in den meisten Fällen so sein wird, damit wir IT-Sicherheit schaffen können und darüber nationale Sicherheit oder gibt es Ausnahmen, zum Beispiel, ich finde eine Schwachstelle in einer Ransomware. Da gehe ich nicht zu den russischen Cyberkriminellen hin und sage: Hey, ich habe eine Schwachstelle bei euch gefunden, wollt ihr die fixen? Es muss eine Möglichkeit geben, einen Prozess aufzusetzen, wo bewertet wird, ob diese Schwachstelle nicht vielleicht auch für einen bestimmten Zeitraum zurückgehalten wird und dann vielleicht für andere Zwecke ausgenutzt werden kann. Hier würde ich aber das BSI nicht aus der Pflicht entlassen. Das BSI muss in einen solchen Prozess eingebunden sein, denn wer, wenn nicht das BSI, soll denn der IT-Sicherheitsfürsprecher in so einem Prozess sein? Von daher kenne ich die BSI-Position, dass man sagt, okay, Coordinated Vulnerability Disclosure, wenn jemand uns meldet, dann geben wir es an die

Produkte weiter. Alles andere wollen wir nicht sehen und nicht hören. Das funktioniert so nicht. Staatliches, umfassendes Schwachstellenmanagement beinhaltet auch, dass man sich dann im Zweifelsfall auch die Finger dreckig machen muss und in einem Prozess die IT-Sicherheitsfahne hochhalten muss, wo man eigentlich lieber nicht drin wäre. Alles Weitere, wie gesagt, in dem Papier für ein staatliches Schwachstellenmanagement von 2018.

AmtVors. **Petra Pau** (Die Linke): Danke schön. Wir sind so gut in der Zeit, dass wir noch eine dritte vollständige Runde machen können, wenn sich alle weiter daran halten, was die Fragezeiten betrifft und natürlich auch die Antwortzeiten. Kollege Hartmann.

Abg. **Sebastian Hartmann** (SPD): Herzlichen Dank. Ich möchte gerne eine Frage zunächst an die Präsidentin des BSI richten. Man merkt Ihre Unabhängigkeit angesichts Ihrer Stellungnahme. Sie schreiben, man sollte den CISO Bund fest beim BSI verankern. Sie wissen, dass in der Bundesregierung dazu unterschiedliche Auffassungen existieren, aber da merkt man, die Unabhängigkeit hat auch damit zu tun, wie man das Amt ausfüllt, wenn ich mir das erlaube. Danke für Ihre Hinweise, mit denen wir uns sehr anfreunden können, um Klarheit in der Sache haben. Sie haben das Verhältnis Bund-Länder jetzt schon in der Verantwortung. Könnten Sie zu diesem, weil es hier öfter angesprochen worden ist, einheitlichen und hohen Sicherheitsniveau in der föderalen Struktur noch einmal ausführen? Können Sie uns das bitte einmal darlegen, wie das jetzt gelingt? Ist das unter einer Verfassungsänderung möglich? Wie stellt man das dar? Denn auch diese NIS-2-Richtlinien-Umsetzung ist ja nun in anderen europäischen Staaten auch nicht sofort angegangen worden, sondern es ist vielfach über Referentenentwürfe gesprochen worden.

Der zweite Punkt, da möchte ich gerne nochmal an Frau Prof. Dr. Schulmann anknüpfen. Sie haben, und das ist jetzt dieser zweite Teil der Diskussion in der Runde gewesen, nochmal Hinweise zur aktiven Cyber-Abwehr gegeben. Oftmals sind jetzt auch Schwachstellen dieses Zusammenspiels erwähnt worden. Ich stelle mir mal vor, wir würden über eine andere deutsche Behörde so reden wie über das BSI, dass sie unabhängig aufgestellt werden soll, mit massiven Eingriffsbefugnissen – schon abstrakte Warnungen vor technischen Produkten können ein Unternehmen in den Ruin treiben! Überlegen wir mal, wir würden eine Sicherheitsbehörde anderer Art so aufstellen, dass sie praktisch völlig frei eingreifen könnte. Wie geht man eigentlich rechtsstaatlich damit um? Gleichzeitig sind wir gefordert als Deutschland. Wie gehen wir angesichts der Zeitenwende damit um, dass es andere Staaten nicht so freundlich mit uns meinen. In China existiert ein Gesetz, das dazu verpflichtet, Schwachstellen eben nicht öffentlich bekannt zu geben, sondern nur dem Staat zu melden, der sie geheim hält. Was sind Ihre Hinweise zur Cyber-Abwehr? Was sind Ihre Hinweise zu Schwachstellen dieser doch so rauen Welt, in der wir uns befinden und in der wir unsere Freiheit auch verteidigen wollen?

AmtVors. **Petra Pau** (Die Linke): Danke schön. Frau Plattner.

SVe **Claudia Plattner** (BSI): Danke schön. Ich sage gerne noch ein paar Worte zum Thema Zentralstelle bzw. wichtiger noch zur Zusammenarbeit zwischen Bund und Ländern. Zwei Aspekte sind mir dabei wichtig. Zum einen haben wir in der Zusammenarbeit an vielen Stellen ein gutes Arbeitsklima. Wir arbeiten an vielen Stellen auch gut zusammen, aber in wirklich wichtigen Punkten eben halt noch nicht. Und da wird uns gesagt, das geht so nicht, zum Beispiel aus verfassungsrechtlichen Gründen. Das ist Punkt Nummer eins. Zum Thema, dass wir für ein gemeinsames Lagebild brauchen: Viele der Informationen, die auch im Rahmen von NIS-2 auflaufen, laufen in den Ländern auf. Die müssen an einer zentralen Stelle zusammenkommen, Stichwort: gemeinsames deutsches Lagebild. Das ist ein Thema.

Zweiter Punkt. Wir haben einiges an Tools, an Schwachstellen-Scan-Tools für Behörden, an Malware-Erkennungen, die man auch zur Verfügung stellen kann. Diese Themen würden wir sehr, sehr gerne auch den Ländern zur Verfügung stellen. Und hier haben wir aber einfach das Problem, dass uns gesagt wird, Mischverwaltung dürfen wir nicht. Und da habe ich immer Schwierigkeiten, das den Menschen da draußen zu erklären, dass wir nicht so zusammenarbeiten können, wie wir zusammenarbeiten müssen, um da wirklich wirksam zu sein.

Zu guter Letzt der dritte Punkt, das

Krisenmanagement und die Krisenvorbereitung. Wir müssen sicherstellen, dass wenn eine große Krise und ein großer Eingriff kommt, dass wir von Sekunde null an eine entsprechende Koordinierungsfunktion im Krisenmanagement haben. Das müssen wir üben. Das geht nicht nur mittels der Amtshilfe, sondern das muss verstetigte Übung sein. Wir müssen uns kennen. Wir müssen das oft genug miteinander durchgespielt haben.

Das sind die Punkte, die uns im Moment aus einer gesamtstaatlichen Sicht nach wie vor viele Probleme machen. Bei der Einheitlichkeit der Umsetzung der NIS-2-Richtlinie haben wir in der Tat das Problem, dass es in verschiedenen Bundesländern auch verschieden gehandhabt wird, oft auch danach ausgerichtet, wie die Ressourcenlage ist. Das kann man absolut verstehen. Das tut der Einheitlichkeit des Cybersicherheitsniveaus aber nicht gut. Wir haben Länder, die sich dort anders und besser aufstellen können. Wir haben aber auch Länder, die das so nicht leisten können. Die würden sehr gerne auch mehr unsere Hilfe in Anspruch nehmen können. Das können wir nicht immer leisten bzw. dürfen wir nicht leisten. Das ist genau das Thema, das uns an dieser Stelle umtreibt. Da sehen wir Arbeitsbedarf.

AmtVors. **Petra Pau** (Die Linke): Danke, Frau Prof. Schulmann.

SVe **Prof. Dr. Haya Schulmann** (Johann Wolfgang Goethe-Universität): Danke für die Frage. Aktive Cyberabwehr – das sind nicht nur Schwachstellen. Es gibt mehrere Methoden. Man kann systematisch Angriffe abwehren oder die Abwehr von Angriffen ermöglichen, auch ohne Eingriff in angreifende Systeme oder Infrastrukturen, sondern durch Angriffe oder Manipulation in der Infrastruktur. Das heißt, Schwachstellen braucht man in vielen Maßnahmen gar nicht. Man kann Angriffe abwehren, ohne dass man die Hackbacks macht oder Schwachstellen ausnutzt.

Zur Frage Schwachstellen. Das ist eine komplexe Frage, ob wir Schwachstellen brauchen. Aus meiner Sicht hat es auch mit digitaler Souveränität zu tun. Wollen wir nur abhängig sein im Bereich Schwachstellen und auch nur von anderen Ländern oder Informationen bekommen, oder wollen wir auch selbst agieren können? Digitale Souveränität ist zurzeit ein wichtiges Thema, auch angesichts der geopolitischen Lage. Wenn wir selbst in diesem Bereich keine Expertise aufbauen, dann sind wir natürlich komplett abhängig von anderen Ländern und werden hoffen, dass sie uns weiterhin unterstützen werden.

Dann zum Thema Schwachstellen. Man muss sie finden, man muss sie suchen. Das bringt mich auch zum Thema Lagebilder und aktiver Cyberabwehr. Lagebilder sind auch ein Mechanismus unserer aktiven Cyberabwehr. Die Lagebilder unterstützen die Abwehr, die Priorisierung von Maßnahmen, die Bewertung der Entwicklungen, die Risiken und können auch die Fragen beantworten: Wie sieht unsere digitale Infrastruktur aus? Wie sieht unsere digitale Souveränität aus? Wo sind die Ressourcen? Wissen wir in der Politik, wenn die Politik Entscheidungen trifft, ob die IT sich in Deutschland oder im Ausland befindet? Wer verwaltet diese IT? Wer hat Zugriff zu dieser IT? Wissen die Parteien das? Wissen die Ministerien das oder die Verwaltungen in den Ländern? Das ist eine wichtige Sache.

AmtVors. **Petra Pau** (Die Linke): Sie müssen zum Punkt kommen.

SVe **Prof. Dr. Haya Schulmann** (Johann Wolfgang Goethe-Universität): Es ist sehr wichtig, dass das BSI eine zentrale Rolle in diesen Dinge, im NIS-2-Umsetzungsgesetz bekommt und das dann als Dienst für Länder und Kommunen anbieten kann. Idealerweise brauchen wir keine Ausnahmen. Alle brauchen das. Ausnahmen erzeugen nur Lücken und machen alles teurer und komplexer.

AmtVors. **Petra Pau** (Die Linke): Kollege Henrichmann.

Abg. **Marc Henrichmann** (CDU/CSU): Danke schön. Ich glaube, festhalten kann man, die Bedrohungslage spitzt sich enorm zu. Die Aufgaben wachsen unendlich an. Frau Plattner, Sie sind eine sehr engagierte BSI-Präsidentin, aber ehrlicherweise muss man sagen, in Stellen und in Geld ist die Wertschätzung bislang bei Ihnen nicht angekommen. Deswegen habe ich zwei Fragen. Einmal an Professor Kob und einmal an Herrn Eisengräber.

Herr Kob, Sie haben in Ihrer Stellungnahme mit Blick auf das BSI und die neuen Aufgaben die Formulierung gewählt, wir bauen auf Unternehmensseite eine nicht zu unterschätzende

Bürokratie auf, die auf staatlicher Seite auf ein Vakuum stößt. Wie sehen Sie die abschließend und zusammengebunden die Handlungsnotwendigkeiten in Sachen Unterstützung BSI? Was sind konkrete Vorschläge?

Herr Eisengräber, zum Lagebild haben Sie schon etwas ausgeführt. Wenn wir davon ausgehen, dass die Haushaltspolitik, so wie wir sie aktuell beobachten, bleibt, dass wir eine desolate Finanzierung aufseiten des BSI fürchten müssen – damit rechnen müssen will ich gar nicht sagen –, dann die Frage, was kann man in Sachen Lagebild tun? Digitalisierung, Harmonisierung, also Bürokratieabbau, auch um die Wirtschaft entsprechend nicht überzubelasten, aber insbesondere: Welchen Beitrag kann die Wirtschaft leisten in Unterstützungsfragen? Beispielsweise MIR-Teams. Wir haben einen kleinen vierstelligen Bereich von KRITIS-Betreibern aktuell. Da ist die persönliche Betreuung denkbar. Das wird bei 30 000 KRITIS-Betreibern so nicht mehr gehen. Welchen Beitrag kann beispielsweise die Privatwirtschaft leisten, um eben da Sicherheit zu gewährleisten?

AmtVors. **Petra Pau** (Die Linke): Herr Professor Kob.

SV **Prof. Timo Kob** (HiSolutions): Die 24-Stunden-Regel zur Meldung macht nur Sinn, wenn ich in schnellster Zeit reagieren muss. Jetzt mache ich den Job 30 Jahre und in 30 Jahren ist es mir nicht einmal passiert – ich bin sicherheitsüberprüft et cetera, habe diverse Rahmenverträge mit dem Bund, et cetera –, nicht einmal habe ich Informationen erhalten, die ich nicht vorher von Heise.de oder wem auch immer kannte. Aber nur, wenn die Chance dazu besteht, dass man in der Vorwarnung – „Achtung, hier ist einem was passiert, du bist ein ähnliches Unternehmen, pass auf“ – nur wenn diese Informationen schnell weitergegeben werden, nur dann hat es Sinn. Wir hoffen auf eine Information-Sharing-Portal. Aber wenn die Aussage ist „Ich gehe das Risiko ein, jemanden zu informieren, der es nicht wissen soll“, und nur das Risiko bewerte, anstatt das Risiko zu bewerten, „Wenn ich die alle nicht informiere, was passiert denn dann?“, dann habe ich an dem Punkt nichts gewonnen. Das ist der reaktive Teil.

Warum verpflichte ich, so schnell zu reagieren? Das ist Stress für Unternehmen. Ich kenne es als Incident Responsler, nach 24 Stunden sind die alle noch in einer Schockstarre und sind nicht in der Lage, überhaupt rauszufinden, ob es ein Vorfall ist. Ist nur die IT kaputt? Geschweige denn rauszufinden, ist der Vorfall denn so bedrohlich, dass ich melden muss? Aber wir haben auch das Proaktive. Wir haben auch das Schwachstellen-Scanning, was nur auf die kritische Infrastruktur bezogen ist. Aber es wäre besser, wenn es auf das gesamte deutsche Internet funktionieren würde. Wir erfahren von einem Zero-Day-Exploit und die Versicherungen sind dann dabei, zu sagen, welcher meiner Klienten ist/kann davon betroffen sein. Die dürfen das. Das BSI darf das nicht. Wer ist betroffen? Wer geht ein Risiko ein, um das zeitnah zu machen? Da vergeben wir uns riesige Chancen.

AmtVors. **Petra Pau** (Die Linke): Danke. Herr Eisengräber.

SV **Boris Eisengräber** (Schwarz Digits): Wie schon erwähnt, erlebe ich die Zusammenarbeit mit dem BSI sehr positiv. Sei es im Rahmen von KRITIS oder der Branchen-Arbeitskreise. Ein Faktor ist hier, dass das BSI von Anfang auch mit KRITIS einen sehr partnerschaftlichen Ansatz mit der Privatwirtschaft gewählt hat. Das ist nur richtig, weil, wie heute schon mehrfach erwähnt, Cybersecurity nur gemeinsam gelöst werden kann. Insofern ist aus meiner Sicht eine Ausweitung der Zusammenarbeit denkbar, um Ressourcen, aber auch Knowhow der Privatwirtschaft besser nutzen zu können. Sei es in der Konsolidierung von Informationen, Berichtswesen, Beratungsleistungen. Das ist grundsätzlich denkbar. Wie auch schon erörtert, das Gesetz liefert nur den erhofften Erfolg, wenn Informationen, Meldungen zeitgerecht verarbeitet und darauf reagiert wird und das BSI dazu befähigt ist. Was auch schon anklang, ist das hohe Vertrauen in die Vertrauensstellung, die das BSI genießt. Das ist ein Faktor, der dort auch berücksichtigt werden muss, wenn man stärker auf Dienste der Privatwirtschaft zurückgreift. Insofern ist es auch ein Punkt, Frau Prof. Schulmann hat es angesprochen, wo wir das Thema digitale Souveränität und Stärkung der digitalen Souveränität beachten müssen.

AmtVors. **Petra Pau** (Die Linke): Danke schön. Kollegin Khan.

Abg. **Misbah Khan** (BÜNDNIS 90 / DIE GRÜNEN): Ich habe eine Frage an Frau Plattner und eine

Frage an Herrn Kipker.

Zuerst an Frau Plattner. Jetzt ist zuletzt in dieser Debatte das Koalitionsvorhaben des effektiven Schwachstellenmanagements angesprochen worden. Können Sie einmal bitte auch in Anbetracht der gegenwärtigen Bedrohungslage durch internationale Aspekte Ihre Sicht auf die IT-Sicherheitsperspektive darstellen zur Schließung von Schwachstellen?

Und an Herrn Kipker: Wir diskutieren jetzt ein bisschen mehr als eineinhalb Stunden. Vielleicht gibt es in der Debatte einen Punkt, von dem Sie meinen, der ist noch zu kurz gekommen. Dann würde ich Sie bitten, den noch zu beleuchten. Danke schön.

AmtVors. **Petra Pau** (Die Linke): Bitte.

SVe **Claudia Plattner** (BSI): Danke schön für die Schwachstellenfrage. Ich glaube, es ist eine ganz wichtige Frage. Wir haben Länder dieser Welt, die haben in der Tat eine ganz klare Strategie, die darauf abzielt, Schwachstellen zu sammeln und diese für staatliche Zwecke einzusetzen, sprich für potenziell Spionage, Sabotage et cetera pp. Wir haben dazu entsprechende Berichte, wir haben entsprechende Erkenntnisse. Wir sehen klar, wie das als politisches Mittel eingesetzt wird. Das heißt, wir müssen davon ausgehen, dass jede Schwachstelle, die es da draußen gibt, auch gegen uns verwendet wird. Deswegen ist uns als denjenigen, die sich um das Thema Schutz der Infrastrukturen und der Firmen und Institutionen kümmern, natürlich ganz wichtig, dass wir möglichst viele, möglichst jede Schwachstelle schließen. Denn jede, die da draußen ist, wird auch gegen uns verwendet. Und bei jeder, die da draußen ist, sollten wir nicht glauben, dass wir die einzigen sind, die sie verwenden können. Insofern plädieren wir stark dafür, natürlich zu schließen. Das ist jetzt aber natürlich auch nur unsere Perspektive. Das ist auch unser Job, genau diese Perspektive einzunehmen. Mir ist vollkommen klar, dass es andere Institutionen in der Bundesregierung gibt, die eine andere Perspektive darauf haben und die auch haben müssen. Das gehört dazu. Nichtsdestotrotz ist unsere Expertenmeinung, aus unserer Perspektive sehr klar, der Schutz. Wir dürfen uns nicht der Illusion hingeben, dass diese Schwachstellen nicht genutzt werden. Wir haben Angriffe auf Parteien in letzter Zeit gehabt. Wir hatten Angriffe auf politische Stiftungen, auf den vorpolitischen Raum. Wir hatten Angriffe auf den Bundestag selbst. Viele von diesen Angriffen haben mit Schwachstellen und sogenannten Zero-Days zu tun und ich plädiere dafür, dass wir einen klaren Prozess haben, bei dem vor allem Forscher sich sicher sein können, dass die Schwachstellen auch geschlossen werden. Da bin ich absolut dafür. Wenn es darüber hinaus den Bedarf gibt, eine weitere Regelung zu treffen für Schwachstellen, mit denen genau das nicht passieren soll, dann werden wir den regeln müssen. Wir könnten aber das vielleicht auch in zwei Stufen machen. Wenn das ein Punkt ist, der uns auffällt, wie gesagt, ist mir wichtig, dass wir das Gesetz in Kraft treten lassen, dann können wir das vielleicht auch in zwei Schritten machen. Danke.

AmtVors. **Petra Pau** (Die Linke): Danke. Professor Kipker.

SV **Prof. Dr. Dennis-Kenji Kipker** (Universität Bremen): Ich würde ganz gerne zwei Punkte noch einmal ansprechen. Einerseits § 30 BSI-Gesetzentwurf. Der liegt mir schon seit längerem schwer im Magen, weil da ja einfach nur die Aufzählung von Möglichkeiten und Maßnahmen abschließend technisch-organisatorischer Art wiedergegeben wird, die zu einem höheren Cybersicherheitsniveau führen sollen. Ich finde diese Vorschrift irreführend, ich finde sie auch schon in der NIS 2-Richtlinie irreführend, weil es eben nahelegt, dass man durch Einzelmaßnahmen ein höheres Maß an Cybersicherheit erreichen könnte und das Risikomanagement an sich außer Acht gelassen wird. Wir sehen auch jetzt schon in der Praxis, dass teilweise Cybersicherheitsunternehmen, Beratungsunternehmen wie auch vor allem Produkthersteller das für sich ausnutzen, indem sie sagen, ja, durch diese und jene Maßnahme bist du am Ende NIS-2-compliant, was bis zum verschlüsselten USB-Stick reichen kann. Das ist ein Problem, wenn wir an die Umsetzung denken. Da sollte man vielleicht überlegen, weil es andere Mitgliedstaaten teils auch so machen, ob man wirklich eins zu eins auf diese Vorschriften referieren muss oder ich einfach sagen kann, wir referenzieren auf den Stand der Technik, wie wir es bislang auch gemacht haben, legen das Ganze aber europarechtskonform aus, ohne das jetzt eins zu eins an der Stelle wiederzugeben. Ich glaube, das würde vielen helfen, weil man dadurch diesen Aspekt des Risikomanagements in den Mittelpunkt stellt

und einige Betriebe, die jetzt neu betroffen sind, teils auch gar nicht die IT haben, um diese Maßnahmen im Einzelnen durchsetzen zu können, die in Artikel 21 Abs. 2
NIS-2 beschrieben werden.

Des Weiteren, abschließend das Thema Begrifflichkeiten. „Wesentliche und wichtige Dienste“, heißt es in der NIS 2-Richtlinie. Wir machen davon eine Ausnahme, indem wir sagen, besonders wesentliche und wichtige Einrichtungen. Da stellt sich die Frage, warum. Es gibt auch durchaus Unternehmen, die in mehreren Mitgliedstaaten tätig sind und da führt das Ganze zur Verwirrung.

Und last but not least, das wird man jetzt nicht abschließend in 30 Sekunden klären können, die Frage, ob wir überhaupt Betreiber kritischer Anlagen in diesem Sinne begrifflich benötigen, weil ja zwischen wesentlichen und wichtigen Diensten auf europäischer Ebene differenziert wird. Und so eine Sonderkategorie kennt das europäische Recht an der Stelle nicht. Und es wird ja sowieso in § 31 des Gesetzentwurfs, glaube ich, gesagt, dass Cybersicherheit risikoabhängig zu gewährleisten ist. Für diese besonderen Kategorien von Unternehmen müsste risikoabhängig sowieso mehr geleistet werden. Da sehe ich nicht zwingend den Bedarf, noch mal in eine Sonderkategorie oder einen Sonderweg hier in Deutschland zu gehen. Danke.

AmtVors. **Petra Pau** (Die Linke): Danke. Herr Janich.

Abg. **Steffen Janich** (AfD): Vielen Dank. Meine zwei Fragen gehen an Frau Plattner. Frau Plattner, glauben Sie, dass alle von dem gesetzbetroffenen Unternehmen von sich aus innerhalb von drei Monaten eine Registrierung beim BSI oder beim BBK vornehmen werden, oder sollte der Staat auf diese Unternehmen zugehen?

Und meine zweite Frage. Wie wird die Erfassung gewährleistet, wie wird die Einpflegung der neuen Daten problemlos ablaufen? Sollen sie dann bei den Behörden eingehen oder läuft die Erfassung auf eine Kommunikation mit dem neuen Partner hinaus, was dann entsprechend arbeitsintensiv werden könnte?

SVe **Claudia Plattner** (BSI): Da versuche ich gerne, etwas zu sagen. Gehen wir davon aus, dass alle Firmen sich innerhalb der ersten drei Monate registrieren werden? Nein. Und wir fußen da schlichtweg auf den Erfahrungswerten, die wir haben. Tatsächlich war es in der Vergangenheit so, dass wir im Zweifelsfall den Firmen dann auch hinterhertelefoniert haben. Wir haben uns also aktiv darum bemüht, dann auch die Registrierung zu bekommen, in dem Maße, in dem wir das tun konnten. Das werden wir bei 29 500 Unternehmen, die wir aktuell schätzen, natürlich nicht schaffen können. Das heißt, wir werden insbesondere vor dem Hintergrund der Ressourcensituation damit leben müssen, dass viele Firmen ein Stück weit durchs Raster fallen. Wir werden uns sicherlich Stück für Stück, nach und nach, auch darum kümmern, aber in den ersten drei Monaten halte ich das für nicht sehr realistisch. Hinzu kommt, dass viele Firmen auch noch gar nicht wissen, dass sie betroffen sind. Wir haben da zwar Angebote geschaffen, sodass sie testen können, ob sie betroffen sind. Das läuft auch gut, das wird auch rege nachgefragt. Nichtsdestotrotz, wenn sich die Firmen damit erst gar nicht beschäftigt haben, haben sie unter Umständen noch nicht mal die Idee, dass sie betroffen sein könnten. Würde ich mir wünschen, dass wir das aktiv können? Ja, das würde ich mir natürlich wirklich wünschen. Wie gesagt, wir versuchen mit den Möglichkeiten, die wir haben, das Bestmögliche umzusetzen. Dann werden wir die neuen Daten problemlos integrieren können. Wir können viele der bestehenden Strukturen bei uns gut verwenden und weiterverwenden. Wir bauen aber natürlich auch jetzt ein Stück weit auch noch neue Dinge auf und vor allen Dingen brauchen wir die europäische Harmonisierung. Da wird es noch einiges an Anpassung geben. Das heißt, wir können auf ein gutes Fundament aufsetzen, aber völlig problemlos wird das auch nicht laufen. Wir sind aber mittendrin in den Vorbereitungen und ich bin durchaus optimistisch, aber wahrscheinlich wird das nicht ganz reibungsfrei ablaufen.

AmtVors. **Petra Pau** (Die Linke): Vielen Dank, Kollege Höferlin.

Abg. **Manuel Höferlin** (FDP): Vielen Dank. Noch einmal eine Frage an Herrn Dr. Herpig im Ansetzen an das, was Sie in Ihrem zweiten Durchgang gesagt haben, nämlich zur Nutzung von Schwachstellen, die berechtigte temporäre Nutzung von Schwachstellen, so will ich es mal zusammenfassen, die Sie beschrieben haben, und die Einbindung in einen Prozess durch das BSI oder nicht.

Ich glaube, die Begründung zu sagen, weil andere Staaten Verpflichtungen haben, Schwachstellen gemeldet zu bekommen, um sie dann gegen beispielsweise uns zu nutzen, erfordert, dass auch wir Schwachstellen melden, um sie dann gegen sie zu nutzen, ist, glaube ich, unsinnig. Da sind sich wahrscheinlich viele hier in dem Raum einig. Frau Plattner sagt auch gerade, solche Schwachstellen schließt man am besten, denn dann können sie nicht mehr gegen uns genutzt werden. Und es ist manchmal, glaube ich, ein bisschen naiv zu glauben, dass wenn wir Schwachstellen finden und sie dann gegen jemand anderen nutzen wollen, dass dann andere nicht auch diese Schwachstelle finden, um sie dann gegen uns zu nutzen. Also die sind auch nicht blöd. Das heißt, entscheidend ist doch das Kriterium, wo ist denn diese Schwachstelle? Also nicht, ist das eine Standardsoftware, ist es eine Lieferkette, ist das etwas, was jeden von uns betreffen kann oder ist das eine Software oder eine Einrichtung, die nur in bestimmten Ländern vorkommt oder wie Sie selbst gesagt haben, Ransomware? Vielleicht führen Sie doch mal aus, wie denn so ein Prozess genauer aussehen kann, aus Ihrer Sicht, unter Einbindung des BSI.

Und das schließt an die Frage an, um das jetzt mal gegenüberzustellen, Frau Plattner: Sie hätten am liebsten, dass Sie nicht in diesen Prozess eingebunden sind. Ich glaube aber, dass es schon gut ist, wenn das BSI zum Beispiel bei der Erstellung von Kriterien eingebunden wäre. Vielleicht können Sie danach einmal darstellen, wie Sie denn gerne eingebunden wären und wo Sie nicht gerne eingebunden wären in solch einem Prozess, also ins operative Doing, um die einzelne Stelle zu bewerten oder in abstrakte Regelungen. Denn ich glaube, das ist ein Punkt, der noch wesentlich fehlt in der NIS-2-Umsetzung und den wir unbedingt brauchen und den wir auch in diesem Zug brauchen, denn es lässt sich nicht abwarten, weil Schwachstellen dauernd ausgenutzt werden. Wir haben kein richtiges Schwachstellenmanagement.

AmtVors. **Petra Pau** (Die Linke): Danke, Sie haben das Wort.

SV **Dr. Sven Herpig** (interface): Wunderbar, besten Dank. Kurze Vorbemerkung: Schwachstellen sind, auch wenn wir das hier gerade in den Mittelpunkt stellen, gerade nicht das Haupteinfallstor für Vorfälle, sondern es sind wirklich Zugangsdaten, die abgefangen und dann immer wieder benutzt werden. Das noch einmal zur Klarstellung.

Ansonsten sind wir uns einig bei diesem Punkt, der gerade vorgebracht wurde. Es handelt sich um einen Edge-Case. Schwachstellen-Ransomware, Schwachstellen in einer fake-russischen Artillerie-App für die ukrainischen Soldaten und so weiter. Da kann man sich zwei Sachen vorstellen. Die simpelste Lösung ist zu sagen, alle Behörden, alle Behördenvertreter müssen Schwachstellen, sofern sie davon Kenntnis erhalten, zeitnah oder umgehend an das BSI melden. Das BSI sorgt sich dann darum, dass die geschlossen werden, zusammen mit den Produktverantwortlichen. Hier muss es aber natürlich die Möglichkeit geben, dass das BSI auch entscheiden kann, die Schwachstelle nicht weiterzugeben, zum Beispiel, weil es eben eine Schwachstelle in einer Ransomware ist, zum Beispiel, weil es ein Produkt ist, was end of life ist, es gibt keinen Produktverantwortlichen mehr, dann kann das BSI sich entscheiden, irgendwen einzustellen, der dann, wenn es Open-Source ist, einen Code schreibt, der die Stelle fixt und so weiter. Aber wir müssen natürlich auch bei der Gesetzgebung dafür sensibel sein, dass es Edge-Cases geben kann, wo das eben nicht immer direkt durchläuft und alles ans BSI geht, das BSI meldet alles, alles wird geschlossen, sondern dass es diese Edge-Cases eben gibt. Der Prozess, wie wir ihn aufgemalt haben, ist in der Tat so, dass Schwachstellen, die nicht direkt geschlossen werden sollen, wo man überlegen soll, ob sie geschlossen werden sollen, in einen Prozess eingeführt werden. Dort wird anhand dieser Kriterien – wo ist sie, wie schwer ist es, sie auszunutzen, muss sie gechained oder verkettet werden mit anderen Schwachstellen, damit es nutzbar ist, wissen wir überhaupt, wer dahintersteckt und so weiter – beurteilt, was mit dieser Schwachstelle geschehen soll, ob sie sie eventuell für einen Zeitraum zurückgehalten wird. In diesem Gremium muss meines Befindens das BSI sitzen und das BSI muss darauf hinwirken, dass in den meisten Fällen, wo man es für sinnvoll erachtet, diese Schwachstelle dann eben auch ans BSI zum Schließen gegeben wird. Wenn das BSI nicht drinsitzt, kann man sich auch das ganze Gremium sparen, denn dann sitzen diejenigen drin, die die Schwachstelle natürlich zurückhalten wollen, dann brauchst du auch keinen Diskurs, dann brauchst du auch keine Kriterien, sondern kannst direkt zurückhalten, und deswegen brauchen wir, wenn wir in diesen etwas

komplexeren Prozess gehen, einen Vertreter, eine Vertreterin mindestens der IT-Sicherheit darin, die darüber entscheiden kann. Man kann auch über Sperrminoritäten nachdenken, man kann über Vetos nachdenken und so weiter.

AmtVors. **Petra Pau** (Die Linke): Das müssen wir jetzt verschieben.

SV **Dr. Sven Herpig** (interface): Es gibt da mehrere Kriterien und das verschieben wir in das Papier hinein.

AmtVors. **Petra Pau** (Die Linke): Frau Plattner.

SVe **Claudia Plattner** (BSI): Sehr gerne. Wir haben in der Diskussion, die wir schon seit einiger Zeit miteinander führen, natürlich angeboten, dass wir als allererstes auch einen Satz an Kriterien erstellen. Den haben wir auch erstellt. Da gehören dann zum Beispiel so Dinge dazu, wie, ob eine Nutzung von „remote“ aus möglich ist, versus, man muss vor Ort sein und ein Stück Technik in der Hand haben, was dann im Zweifelsfall auch sehr viel größeres Schadpotenzial hat. Und es gibt natürlich dann auch noch jede Menge Fälle, die sich irgendwo im militärischen Bereich abspielen. Man kann dafür eine Liste von Kriterien erstellen. Das haben wir getan. Und das ist dann natürlich auch immer zur Verfügung zu stellen. Wir hatten vorgeschlagen oder zumindest positiv diskutiert, dass auch wir sehen, dass man dafür ein Gremium hat, das entsprechend solche Entscheidungen trifft. Wir hatten angeboten, dieses Gremium aus unserer Perspektive mit den notwendigen Kriterien zu versorgen. Und wir hatten auch angeboten, dass wir unter Umständen vielleicht alle ein, zwei Jahre dann im Nachgang auf die Schwachstellen zurückblicken und man gegebenenfalls Kriterien nachschärft, einfach aufgrund der Lessons Learned mit den Erfahrungen, die man da gesammelt hat. Das haben wir angeboten. Dazu stehen wir auch nach wie vor. Bei der Frage, ob wir in diesem Gremium mit dabei sein sollten oder nicht, würden wir im Moment erst mal dafür plädieren, dass das auch ohne uns geht. Die Diskussion kann man aber natürlich auch einfach fortsetzen. Wir glauben, dass man da auch gute Lösungen finden kann. Das wäre meine kurze Antwort.

AmtVors. **Petra Pau** (Die Linke): Vielen Dank. Ich schaue jetzt in die Runde. Quält irgendeine Fraktion noch eine Frage? In Ordnung. Dann danke ich allen Beteiligten, den Sachverständigen genauso wie den Abgeordneten. Sie sehen, wir sind auch in der Lage, diese Ausschusssitzung geordnet und im Zeitplan ablaufen zu lassen. Die Kolleginnen und Kollegen wissen, worauf ich anspiele. Also dann bis Mittwoch. Ich schließe die Sitzung.

Schluss der Sitzung: 12.49 Uhr

Petra Pau, MdB
Amtierende Vorsitzende

Deutscher Bundestag

Ausschuss für Inneres und Heimat

Ausschussdrucksache
20(4)523 A

HISOLUTIONS

STELLUNGNAHME ZUR EXPERTENANHÖRUNG ZUM NIS2UMSUCG

1. Vorbemerkungen

Es ist von höchster Bedeutung, dass dieses Gesetz schnellstens verabschiedet wird. Die Tatsache, dass die Wirtschaft die Einführung fordert, obwohl es zu Mehraufwänden führen wird, spricht hier eine deutliche Sprache. Es besteht die große Sorge, dass sich eine weitere Verzögerung ergibt.
Ziele und Grundidee sind komplett richtig: Was fachlich gefordert wird, sollten alle machen, egal ob reguliert oder nicht.

2. Allgemeine Kritikpunkte

2.1. Rahmenbedingungen

Losgelöst von einzelnen Paragraphen ist zuallererst die zeitlich und inhaltlich fehlende Koordinierung mit dem KRITIS-Dachgesetz problematisch. Hier läuft der Prozess noch schleppender und unerfreulicher als beim hier betrachteten Gesetz. Der erste Entwurf wurde veröffentlicht, ohne jemals mit der Wirtschaft gesprochen zu haben, die Qualität merkte man dann zum Beispiel daran, dass das Wort „Cyber“ im ersten Entwurf des KRITIS-Dachgesetzes nicht einmal vorkam (auch wenn Cybersecurity nicht im Fokus des Gesetzes steht, ist eine vollständige Ausblendung weltfremd und kontraproduktiv).

Noch schlimmer wird es, wenn dann parallel eine dritte Abteilung aus dem BMI „Eckpunkte für eine nationale Wirtschaftsschutz-Strategie“ veröffentlicht. Auch dies offensichtlich nicht abgestimmt und zwar nach meiner Kenntnis weder mit der Wirtschaft noch mit den anderen Abteilungen des BMI.

Aus politischer, verwaltungstechnischer und juristischer Sicht mag dies sinnvoll oder zumindest nachvollziehbar wirken, aus Sicht der betroffenen Unternehmen ist dies mehr als ärgerlich, denn für diese gehören die Themen unauflösbar zusammen.

Es ist Common Sense, dass ein All-Gefahren-Ansatz gewählt werden muss – Deutschland wählt hingegen einen zersplitterten Weg.

Es rächt sich hier in meinen Augen, dass es – brutal gesagt – nichts gibt, was wirklich den Namen Strategie verdient: Egal ob Digitalisierungsstrategie, Nationale Sicherheitsstrategie, Nationale Cyber-Sicherheitsstrategie, Wirtschaftsschutzstrategie: Vision/Mission, SMARTE Ziele (spezifisch, messbar, attraktiv, realistisch, terminiert), abgeleitete konkrete Maßnahmen mit Verantwortlichkeiten und dies alles integriert, übergreifend und in dem Aspekte und Maßnahmen von innerer und äußerer Sicherheit, Finanz- und Industriepolitik, Bildung und Forschung orchestriert: überall Fehlanzeige. Stattdessen Willensbekundungen, Absichtserklärungen und Übersichtspapiere, die nicht ineinandergreifen.

Ein Beispiel für dieses nicht-kohärente Handeln: Wir unterhalten uns meist über die Gefahr des „Gold-Platings“, des Überziehens der europäischen Anforderungen bei der Umsetzung in deutsches Recht, hier haben wir auch einmal die gegenteilige Variante: In Artikel 24 Abs. 1 Satz 2 der originalen NIS-2-Richtlinie heißt es: „Darüber hinaus fördern die Mitgliedstaaten, dass wesentliche und wichtige Einrichtungen qualifizierte Vertrauensdienste nutzen.“

Dies findet sich in der deutschen Umsetzung nirgends wieder, stattdessen kann das Organisationskonto nicht genutzt werden und wird im Gesetz nicht adressiert, die Haushaltsmittel für die eID werden gestrichen und es droht, dass nicht nur in 2025 keine Weiterentwicklung

stattfindet, sondern ab 2026 sogar die Nutzung der laufenden Verfahren gestoppt werden muss, da die Mittel fehlen.

Das ist das Gegenteil eines strategisch sinnvollen, kohärenten und ganzheitlichen Herangehens.

2.2. Geburtsfehler in Brüssel

Zentrale Fehler sind aus meiner Sicht bereits im Vorfeld, also während des europäischen Gesetzgebungsprozesses geschehen. Dies bezieht in meinen Augen Politik, Wirtschaft und Verbände ein.

Viele hatten offensichtlich – ggf. ermüdet durch den zähen Prozess rund um das IT-Sicherheitsgesetz 2 – den seitens der französischen Regierung aufgebauten Zeitdruck unterschätzt, die dies in ihrer Ratspräsidentschaft umsetzen wollten, welche wiederum durch die parallel stattfindende Präsidentenwahl de facto noch weiter verkürzt war. Vielleicht waren wir uns alle auch zu selbstgewiss, dass wie bei NIS1 die deutschen Muster durch die vorlaufende deutsche Gesetzgebung auch wieder zur Blaupause der EU-Regelungen werden würden.

Es gab dann irgendwann einen Weckruf seitens des BMI auch mit Bitte um Unterstützung durch die Wirtschaft(sverbände) in Brüssel, was u. a. dazu führte, dass das Wirtschaftsforum der SPD und der Wirtschaftsrat der CDU wortgleiche Warnbriefe z. B. an die MdEPs versendeten. Dies führte aber nur noch sehr eingeschränkt zu Erfolgen. Die Erfolge lagen dann unglücklicherweise eher in der Rücksichtnahme auf Aspekte des Föderalismus, als etwa auf Aspekten der deutschen Unternehmensstruktur, Stichwort „Mittelstand als Rückgrat der Wirtschaft“.

Die zentralen Kardinalsfehler sind aus meiner Sicht:

- keine Umsetzungsfristen für die in den Anwendungsbereich fallenden Einrichtungen
- Scope zu breit
- Meldefrist von 24 Stunden nicht angemessen

Um nicht falsch verstanden zu werden: Die inhaltlichen Anforderungen von NIS2 sind, wie schon in den Vorbemerkungen unterstrichen, komplett richtig und eigentlich etwas, was für alle Unternehmen, ob von NIS2 betroffen oder nicht, Gültigkeit haben sollte. Realistisch betrachtet sind diese aber von einem großen Teil der Unternehmen noch nicht annähernd vollständig umgesetzt. Jetzt müssen 30.000 Unternehmen dies zeitgleich umsetzen und vermutlich großteils auf Berater zurückgreifen. Diese Berater gibt es aber ebenfalls nicht in der benötigten Anzahl, denn der Stellenmarkt ist leergefegt. Und ob die sprichwörtliche Molkerei mit 51 Mitarbeitern im Allgäu wirklich für Wohl und Wehe unserer Gesellschaft wichtig ist, lasse ich offen.

Am Ende wird vermutlich Folgendes passieren: Es werden Regeln geschaffen, die nur teilweise oder gar nicht umgesetzt werden und die Ausrede, dass der Markt gar nicht die Ressourcen hergab, werden alle ziehen können, die kleine Molkerei sowie der große Energieversorger. Zumindest den Letztgenannten hätte man dieses Schlupfloch entziehen müssen (und hier auch eventuelle Fristen, in denen nicht geprüft wird, verkürzen können).

Auch angesichts der Zeitenwende wäre die Fokussierung auf die wirklich relevanten Elemente effektiver gewesen. Nun erhöhen wir den Deich überall gleichzeitig um wenige Zentimeter, anstatt an den neuralgischen Punkten, die wir ja kennen, schnell massive Verbesserungen zu erreichen.

Eine risikoorientierte Erweiterung auf etwa 10.000 Unternehmen wäre aus der Gesamtbetrachtung zielführender gewesen. Und die Verwendung der eben nur begrenzt vorhandenen Ressourcen dadurch punktgenauer. Nun können wir nur hoffen, dass es der Markt regelt: in dem Sinne, dass die wirklich relevanten Unternehmen bereit sind, höhere Tagessätze zu bezahlen und so die Mittelständler „ausstechen".

Eine Konjunkturhilfe für Sicherheitsberatungsunternehmen wie meines, die diese Branche nicht gebraucht hätte.

Stattdessen wurde in Deutschland dafür mit der dreijährigen Frist der Nicht-Prüfung ein Kunstgriff gewählt. Dies ist einerseits nachvollziehbar und für deutsche Verhältnisse geradezu elegant; man hätte bei den wirklich neuralgischen Punkten lieber auf diese Schonfrist verzichtet, ihnen dafür aber auch einen weniger überforderten Ressourcenpool geboten.

3. Konkrete Kritikpunkte am Gesetzesentwurf

3.1. Nicht akzeptable Reduktionen auf staatlicher Seite

Von Referentenentwurf zu Referentenentwurf zu finaler Fassung wurde die Liste der von den Vorschriften ausgenommenen Institutionen auf staatlicher Seite immer länger und die Liste von umzusetzenden Punkten immer kürzer.

Als erstes fielen auf Empfehlung des IT-Planungsrates die Kommunen und Gemeinden heraus. In den letzten Jahren hat sich gezeigt: „The weakest link" ist auf der öffentlichen Seite und zwar genau die kommunale Ebene, wie Anhalt-Bitterfeld, Schwerin, Südwestfalen-IT etc. gezeigt haben. Und genau diese werden ausgenommen.
Wichtig ist an diesem Punkt: Ein Großteil der Kommunen und Gemeinden WOLLTE reguliert werden, es ist am Ende eine Frage, wer es zahlen muss. Jetzt ist es geklärt: Die nun nicht zu vermeidenden Schäden zahlen wir alle.

Es gibt nur eine Variante, die teurer ist, als jetzt einen Plan zu entwickeln und umzusetzen, um genau diese Schwächsten, aber für die Gesellschaft und Wirtschaft massiv wichtigen Elemente zu schützen: nichts tun.

Und genau dieser Weg wird beschritten.

Man muss konzedieren, dass es tatsächlich unmöglich wäre, die Erfüllung aller Regelungen fristgerecht zu erreichen. Aber daran hat sich bei der Wirtschaft ja auch niemand gestört. Und wenn man Kommunen und Gemeinden nicht per NIS2-Umsetzung schützen kann, so wäre es das Mindeste gewesen, einen einheitlichen und konkreten Handlungsplan aufzusetzen, wie dieses Ziel bis wann in einheitlicher Qualität erreicht werden kann. Nun verbleibt dies bei den Bundesländern mit absehbar sehr unterschiedlichen Ansätzen, die, auch durch Größe und Finanzkraft der Bundesländer geprägt, unterschiedliche Qualität haben werden.

Das zu erwartende Ergebnis haben wir exemplarisch im letzten Jahr beim Thema iKfz (digitalisierte KfZ-Anmeldung) erlebt. Ein bundesweit standardisierbares Verfahren wurde in rund 500 Varianten eingeführt, die jeweils getrennt geschützt werden mussten, was angesichts mangelnder Auditoren unmöglich war und dazu führte, dass das Verfahren in weiten Teilen Deutschlands zwischenzeitlich wieder gestoppt werden musste.

Ich maße mir definitiv keine rechtswissenschaftliche Kompetenz an und dies erst recht nicht auf dem Gebiet des Verfassungsrechts, aber für mich hat dies durchaus auch etwas mit der angestrebten „Gleichwertigkeit der Lebensverhältnisse“ zu tun, wenn es Gegenden gibt, wo die gesamten kommunalen Serviceleistungen über Monate aufgrund mangelnder Vorsorge durch Cyberangriffe nicht zur Verfügung stehen und sich dies mittelfristig auch mit der Wirtschaftskraft der Regionen korrelieren lässt.

Der gleiche Effekt ist auch bei den jeweiligen Umsetzungen auf Länderebene zu erwarten. Unterschiedliche Umsetzungen, mal als Gesetz, mal als Verordnung, mal als Runderlass. Wer prüft die Passgenauigkeit und qualitative Vergleichbarkeit? Vom bürokratischen Aufwand für überregional tätige Unternehmen ganz zu schweigen.

Mit dieser Entscheidung war klar, dass das Gesetz auf staatlicher Seite schon einmal nicht zu einem wirklichen Cybersicherheitsstärkungsgesetz werden konnte.

Aber es kam noch schlimmer, mit der letzten Version haben wir nun definitiv ein Cybersicherheitsschwächungsgesetz. Als letztes fielen die nachgelagerten Bundesbehörden mehr oder weniger heraus. Nachgelagerte Bundesbehörden müssen nicht mehr IT-Grundschutz umsetzen, was heute mit dem UP Bund noch Pflicht ist (§44).
De facto stellt dieser Punkt im Endeffekt sogar die „Netze des Bundes“ infrage, da alle nachgelagerten Behörden eigentlich nicht mehr die Sicherheitsanforderungen für ein einheitliches Sicherheitsniveau erfüllen.

Ein kurzer Einschub zum Thema IT-Grundschutz: Wichtig ist mir der Hinweis, dass Kritik am IT-Grundschutz ob des zu großen Umfangs, fehlender Flexibilität und damit zu hohen Umsetzungsaufwänden nur in geringem Maße treffend ist. Zum einen gilt auch hier ein risikoorientierter Ansatz, der es eben nicht darauf anlegt, dass alle Inhalte erfüllt werden müssen, zum anderen gibt es auch hier immer die Möglichkeit, sinnvolle Alternativwege zu beschreiten. Das BSI ist hier in einem unverschuldeten Dilemma: Entweder werden Hilfen/Umsetzungsleitfäden etc. als nicht konkret genug empfunden, und wenn sie dann konkret genug sind, wird zu großer Umfang und zu wenig Flexibilität moniert.

Darüber hinaus arbeitet das BSI derzeit intensiv an einer massiven Straffung der Inhalte.

§29 ist ein Horrorkabinett für alle sicherheitsaffin denkenden Personen:

- Ausnahme von der Pflicht aus §30 zu Risikomanagementmaßnahmen (außer Bundeskanzleramt und Ministerien)
- keine Billigungs-, Überwachungs- und Schulungspflicht für Amtsleitungen, wie in §38 für Geschäftsleitungen verpflichtend eingeführt (Warum sind Schulungen für Vorstände zwingend erforderlich, für Amtsleiter aber entbehrlich?)
- Ausnahme von Aufsichts- und Durchsetzungsmaßnahmen durch das BSI aus §61 (was auch die Frage nach einem „Bundes-CISO“ noch spannender macht, dazu später mehr)
- Dass Ausnahmen von Bußgeldvorschriften für Amtsleitungen gemacht werden, ist unvermeidbar, verstärkt aber in der Wirtschaft den Eindruck, dass in allen Belangen unterschiedliches Maß angelegt wird.

Aber auch das ist noch nicht alles. Weiterhin ausgenommen sind:

- IT-Dienstleister, die Dienste für Landes- und Kommunalverwaltungen erbringen,
- „Institutionen der sozialen Sicherung“, Bundesbank, Auswärtiges Amt, Bundeswehr, BND, BfV.
- Der Sektor Forschung wird gemäß der Begriffsdefinition „Forschungseinrichtung“ auf angewandte Forschung mit kommerziellem Zweck begrenzt. Warum keine Grundlagenforschung, also genau der Bereich, wo wir in Deutschland aktuell noch wirklich gut aufgestellt sind? Gleiches gilt für durch den Bund finanzierte Forschungseinrichtungen, welche in der Rechtsform einer Stiftung des öffentlichen Rechts nach Landesrecht aufgebaut sind. Ich verstehe, dass dem Bund hier teilweise die Hände gebunden sind. Das Dumme ist nur: Dem Angreifer sind sie nicht gebunden.

3.2. Rolle und Möglichkeiten des BSI

Grundsätzlich ist die Aufwertung des BSI positiv zu bewerten, auch das Streben nach einer Zentralstellen-Funktion ist wünschenswert. In aller Deutlichkeit: Man wird lange nach einem Experten außerhalb von Behörden suchen müssen, der dem Aspekt des Föderalismus bei der Cybersicherheit in der in Deutschland betriebenen Umsetzung etwas Positives abgewinnen kann (gleiches gilt übrigens für die Themen Digitalisierung und Bildung).

Inhaltsleer ist leider auch §48, der das Amt des Koordinators für Informationssicherheit definiert (was inklusive der inoffiziellen Aussagen, dass dieses beim BSI angesiedelt sein soll, absolut begrüßenswert ist).

Aber welche Rechte und Pflichte sind damit verbunden? Aktuell klingt es nach einem zahnlosen Tiger und reiner Symbolpolitik.

Verstärkt wird es noch dadurch, dass in §29 ja explizit die Aufsichts- und Durchsetzungsmaßnahmen aus §61 ausgehebelt werden. Damit ist eigentlich klar, dass die Rolle eines „Bundes-CISOs“ eher Feigenblatt als „Game Changer“ sein wird. Auch hier hätte ein Austausch mit der Wirtschaft geholfen: All diese Fehler hat die Wirtschaft vor vielen Jahren ebenfalls begangen und lernen müssen, dass es so nicht gut funktioniert.

Erforderlich ist hier aus fachlicher Sicht eine klare Weisungsbefugnis, denn das, was zuvor als Expertenmeinung zur aktuellen Ausprägung des Föderalismus in Bezug auf Kernfunktionen der Cybersicherheit postuliert wurde, gilt in gleichem Maße für das Prinzip der Ressortunabhängigkeit.

Wir brauchen keinen Koordinator, der weiß, dass jeder „sein eigenes Ding macht“, sondern jemanden, der diesem Treiben ein Ende bereitet.

Wenn man die „Best Practices“ aus der Privatwirtschaft auf die Rolle eines Bundes-CISOs überträgt, ergibt sich folgende Beschreibung:

Der Bundes-CISO

- koordiniert das Informationssicherheitsmanagement des Bundes,
- entwickelt und pflegt Programme zur Gewährleistung der Informationssicherheit des Bundes im Benehmen mit den Behörden,
- beaufsichtigt die Umsetzung,
- hat ein direktes Vortragsrecht vor dem Innen- und Haushaltsausschuss des Deutschen Bundestages.

Zusätzlich wäre die verpflichtende Einbindung in alle Gesetzesvorhaben etc., die die Cybersicherheit tangieren, sinnvoll.

Viel dramatischer als diese Ausführungen zum Bundes-CISO ist aber die Tatsache, dass dem BSI neue Aufgaben übertragen wurden, dies aber nicht annähernd in der Haushaltsplanung berücksichtigt wurde.

Statt des erforderlichen Aufwuchses stehen 37 Millionen Euro weniger in der Planung und dementsprechend natürlich auch keinerlei neue Stellen.

Wie will man also die 30.000 Unternehmen prüfen, ob deren Registrierung korrekt ist?
Wie prüfen, ob sich Unternehmen nicht registriert haben (hierzu später noch mehr)?
Wer soll den Unternehmen bei Fragen zur Seite stehen?

Und vor allem: Wer soll die einkommenden Meldungen auswerten und Informationen zur Verfügung stellen?

Zur Verdeutlichung: Die Erstmeldung hat gemäß EU-Template 19 Felder, die 72h-Meldung 35 Felder (davon 19 neu), die Abschlussmeldung (44 Felder, davon 9 neu), egal welche Unternehmensgröße betroffen ist. Diese Informationen müssen aber ausgewertet und verarbeitet werden, damit der damit verbundene Bürokratieaufbau einen Sinn ergibt.

Wir bauen hier auf der Unternehmensseite eine nicht zu unterschätzende Bürokratie auf, die dann auf staatlicher Seite auf ein Vakuum stößt.

Die Verarbeitung der Meldungen zu verwertbaren Informationen an die Unternehmen ist aber nur der eine Hebel zur wirklichen Steigerung der Sicherheit.

Der zweite Hebel ist die in §15 definierte Möglichkeit zur Detektion von Angriffsmethoden und von Sicherheitsrisiken. Leider wird hier nur der halbe Schritt gegangen, in dem dies auf die von NIS2UmsuCG betroffenen Institutionen beschränkt wird. Zielführender wäre hier ein Verzicht auf die Beschränkung auf kritische Infrastrukturen, (besonders) wichtige Unternehmen und Verwaltung.

Gerade beim Bekanntwerden einer neuen Schwachstelle beginnt regelmäßig ein „Rat race“ zwischen Angreifern und Verteidigern, um potenziell Betroffene zu identifizieren. Es wäre in diesem Rennen ein wirklicher „Game Changer“, wenn hier das BSI flächendeckend unterstützen könnte.

Dies hat ja auch nichts mit dem Ausnutzen von Schwachstellen zu tun. Claudia Plattner beschrieb das plastisch auf der IT-Sicherheitsmesse it-sa in diesem Monat mit einem „Rundgang, um zu schauen, ob Türen offenstehen“ und eben nicht dem Durchschreiten oder gar Aufbrechen der Tür. Alle Regeln zur Kontrolle dieser Aktivitäten sind ja korrekt und angemessen im Gesetz hinterlegt. Wenn diese gelten, spricht nichts gegen eine Ausdehnung des Betrachtungsbereiches.

3.3. Der Registrierungs- und Meldeprozess sowie Meldepflichten

Betroffenheitsklärung: Bringschuld des Staates, nicht der Unternehmen

Es ist vollkommen unverständlich, warum man es den Unternehmen überlässt, ihre Betroffenheit festzustellen und diese zu melden.
Ein Gesetz, bei dem der Staat sich außer Lage sieht, selbst zu definieren, wer betroffen ist und die Betroffenen zu informieren, hat aus meiner Sicht schon einen massiven Geburtsfehler.
Ebenso ist unklar, warum dies Ländern wie Kroatien und Lettland möglich ist, den deutschen Behörden aber nicht.
Und nein, es ist in vielen Fällen nicht so einfach, die eigene Betroffenheit festzulegen, die Tücke steckt da im Detail.

Auch hier ist der zu erwartende Effekt schon jetzt klar und wird offen diskutiert: Diverse Anwälte und Justiziare empfehlen bereits jetzt, sich im Zweifelsfall lieber nicht zu registrieren, weil man dann sagen kann, dass man es anders bewertet hat und nicht zugeben muss, „sehenden Auges“ gegen Regeln verstoßen zu haben.

Die Komplexität der Regeln bietet genügend Potenzial für derartige Ausflüchte.

Denkbar wäre ein Zwischenweg, wie ihn Italien wählt: Die Unternehmen melden sich in Kurzform, die Behörde prüft die Betroffenheit, nach Bestätigung durch die Behörde startet die Frist, in der die Unternehmen die vollständige Registrierung durchführen müssen.

Das Information Sharing-Portal ist sinnvoll. Wenn es umfassend integriert ist.

Der Ansatz des Information Sharing-Portals ist positiv, sollte aber integriert Cyber- und physische Gefahren abbilden und tagesaktuell sein. Dies führt dann zur Forderung eines gemeinsamen Meldewesens mit dem KRITIS-Dachgesetz.
Und auch wenn dies in erster Linie diesen Gesetzentwurf betrifft, also nicht integraler Bestandteil dieser Anhörung ist, so kann man die Punkte auch nicht völlig voneinander trennen: Dem BSI fehlen die Ressourcen, um eine wirklich funktionale Melde- und Informationsplattform bieten zu können.
Die Aufgaben des BBK (das hiermit explizit nicht kritisiert werden soll!) sind lt. Eigendarstellung:

- Selbstschutz
- Warnung der Bevölkerung
- Schutzbau
- Aufenthaltsregelung
- Katastrophenschutz nach Maßgabe des § 11 ZSKG
- Maßnahmen zum Schutz der Gesundheit
- Maßnahmen zum Schutz von Kulturgut

Was davon ist auch nur annähernd mit der dort angedachten Meldestellenfunktionalität vergleichbar oder auch nur ein guter Startpunkt dafür?
Sprich, wir wollen hier etwas aufbauen, wofür nicht nur Personal, sondern jegliche Vorerfahrung fehlt und was nicht wirklich zur eigenen Grundausrichtung passt. Und dies in einer Situation, in der die integrierte Betrachtung losgelöst von der behördlichen Zuständigkeit absolut zwingend erforderlich ist.

Die Bündelung der Verantwortlichkeit (kombiniert mit der Finanzierung der entsprechend erforderlichen Stellen) erhöht massiv die Qualität und reduziert die Aufwände für Unternehmen (und durch Synergieeffekte auch für die Verwaltung). Eine Win-Win-Situation, die wir einfach an uns vorbeiziehen lassen.

Dies alleine würde aber auch noch nicht für ein wirklich nutzenoptimiertes Informationsportal sorgen.

Eine gute Informationsbasis ist keine Tool-, sondern eine Mindset-Frage.

Aus eigener Anschauung: Mein Unternehmen ist geheimschutzbetreut, in der Allianz für Cybersecurity für zusätzlichen Austausch vertraulicher Informationen „freigeschaltet", dennoch fällt mir kein einziger Fall ein, in dem wir von staatlicher Seite Informationen erhalten haben, die wir nicht schon kannten – meist reicht das Lesen von heise.de aus, also nicht einmal besonderer, nur Experten bekannten / zugänglichen Informationsquellen.

Die Plattform allein löst nicht das Problem, wir brauchen einen Paradigmenwechsel:

Aktuell wird das Risiko bewertet, wenn eine Information einen Unberechtigten erreicht. Nicht bewertet wird aber das oft signifikant höhere Risiko, wenn eine Information die Berechtigten NICHT erreicht. Hier braucht es Regeln und einen Mindset-Wechsel hin zu einem „Mehr und schneller".

Ärgerlich auch, dass derzeit beim Portal nicht die Möglichkeiten des Organisationskontos genutzt werden können (konkret Modul 6 des Organisationskontos), dies würde massive Ersparungen für Staat und Wirtschaft bedeuten. Ein schönes Beispiel, wo langsame Digitalisierung der Verwaltung und Budgetrestriktionen in kürzester Zeit zu Mehraufwänden führen, respektive reale Einsparungen verhindern. Nichtsdestotrotz sollte die zeitnahe Umsetzung und Nutzung des Organisationskontos explizit weiterverfolgt und eingefordert werden. Es ist nicht vermittelbar, warum Unternehmen jetzt einen weiteren „Account" für ihre Interaktion mit staatlichen Stellen haben sollen, wenn das Organisationskonto im Onlinezugangsgesetz eigentlich als zentrale Schnittstelle von Staat und Wirtschaft angelegt ist. Sinnvoll wäre zumindest in der Zwischenzeit für Konzerne auch die Schaffung eines „Oberkontos", das für mehrere meldungspflichtige Tochterunternehmen gilt, um hier den Pflegeaufwand zu minimieren.

Zu kurze und missverständliche Fristen

Aus meiner beruflichen Praxis sind die 24 Stunden bis zur ersten Meldung für viele, gerade kleinere Unternehmen („kleinere" ist hier nicht im Sinne der KMU-Regelungen zu verstehen) zu kurz. Verschärft wird dies durch die uneindeutige Formulierung in § 32 Abs. 1 Nr. 1 BSIG-E:

> 1. „unverzüglich, spätestens jedoch innerhalb von 24 Stunden nach Kenntniserlangung von einem erheblichen Sicherheitsvorfall,…"

Da Unternehmen zunächst prüfen müssen, ob ein Sicherheitsvorfall die Erheblichkeitsschwelle überschreitet, muss zwingend klargestellt werden, dass die 24-stündige Frist zur Abgabe einer Erstmeldung erst NACH Abschluss der Prüfung, ob ein Cybersicherheitsvorfall erheblich ist, beginnt und wann diese Prüfung spätestens beginnt.

Es sollte klarer kommuniziert werden, dass man die Anfangsbewertung eines Vorfalls "zeitnah" durchzuführen hat, jedoch nur innerhalb der Arbeitszeit. Damit würde ein am Samstag festgestellter Vorfall eventuell (und spätestens) am Montagmorgen bewertet, frühestens also am Dienstag zum Ablauf der 24 Stunden führen, sofern die Bewertung einen erheblichen Sicherheitsvorfall feststellt.

Die aktuelle Formulierung könnte indes dahingehend interpretiert werden, dass die 24-Stunden-Frist ab dem Zeitpunkt beginnt, an dem die betroffene Einrichtung von einem Sicherheitsvorfall erfährt. Dies würde de facto zur Pflicht einer 24*7-Verfügbarkeit verschiedener Mitarbeitergruppen führen, was zumindest für kleinere Unternehmen schwer tragbar ist.

Zwischenmeldungen auf ein angemessenes Maß beschränken

Auch nach dieser Erstmeldung wird es nicht gerade besser und vor allem nicht bürokratiearm. Reichte beim IT-Sicherheitsgesetz 2 eine Meldung pro Vorfall, so reden wir jetzt von bis zu fünf Meldungen.
Noch einmal: Für einen Großkonzern mag dies alles machbar sein, wir reden hier aber von der Ausdehnung auf mittlere Unternehmen. Für Unternehmen mit 50 bis 249 Mitarbeitenden wäre es daher wünschenswert, sie zumindest von den Zwischenmeldungen zu befreien. Hier ist einfach auch nicht mit einem Erkenntnisgewinn zu rechnen, der anderen Unternehmen zeitnah zur Verfügung gestellt werden könnte (mal ganz losgelöst von der Frage, wie denn eine zeitnahe Information seitens des BSI gewährleistet werden soll). Aufwand und Mehrwert stehen hier in einem Missverhältnis. Eine andere Möglichkeit wäre, zumindest den Umfang auf ein angemessenes Maß reduzieren oder auf ausgewählte Fälle zu beschränken. Hier könnte die Unternehmensgröße oder die Vorfallsart eine Rolle spielen.

3.4. Der blinde Fleck: Vertrauenswürdigkeitsüberprüfung von Mitarbeitenden

2023 berichtete u. a. der SPIEGEL über die sog. „Vulkan Files“, in der auch für die breite Öffentlichkeit ein Fakt sichtbar wurde, vor dem Fachleute schon lange warnen: Wir müssen neben IT und Physik mehr auf die Menschen schauen. An diversen Stellen u. a. bei Amazon Webservices und Siemens waren in Westeuropa Administratoren beschäftigt, die mit dem russischen Militärnachrichtendienst GRU und dem Auslandsnachrichtendienst SWR in Verbindung gebracht werden konnten.

Spitz formuliert: Selbst sichere IT und sicherer physischer Schutz sind nur Pseudo-Sicherheit, wenn die Personen, die berechtigt Zugang zu IT-Systemen und Infrastrukturen erhalten, nicht auf ihre Vertrauenswürdigkeit überprüft werden können.
Dieser Aspekt wurde sowohl bei NIS2 als auch beim KRITIS-Dachgesetz komplett außenvorgelassen.

Es muss dringend eine Lösung gefunden werden, die es Unternehmen ermöglicht, für einen engen Personenkreis an neuralgischen Punkten Sicherheitsüberprüfungen durchführen zu lassen, die auf dem Prinzip der Freiwilligkeit und entsprechend den Prinzipien und Verfahrensweisen der Sicherheitsüberprüfung nach Sicherheitsüberprüfungsgesetz basieren und von den Unternehmen bezahlt werden.

3.5. Sonstige Kritikpunkte und Verbesserungsvorschläge

Klärung der Situation in der „Karenzzeit“

Wie in den Einführungsbemerkungen erwähnt, ist die Gewährung einer dreijährigen Frist, in der auf Überprüfungen durch das BSI verzichtet wird, eine zumindest auf den ersten Blick elegante Lösung für den Umgang mit der in Brüssel schlicht versäumten Definition einer Umsetzungsfrist.

Bei genauerem Betrachten entstehen aber Fragen, die der Gesetzgeber unbedingt im Vorfeld klären sollte:
Was passiert, wenn in diesen 3 Jahren Sicherheitsvorfälle auftreten und das betroffene Unternehmen noch keine vollständige Umsetzung erreicht hat, zu dem es ja nach Gesetz von Tag 1 an verpflichtet ist?
Werden Cyberversicherungen dann noch zahlen? Werden Richter Schadensersatzzahlungen verfügen mit dem Hinweis auf Nicht-Erfüllung des Gesetzes?

Hier sollte eine Klarstellung im Gesetz erfolgen. Denkbar wäre, dass im ersten Schritt neben der Definition der Verantwortlichkeiten und der Etablierung der Meldestruktur zwingend ein konkreter Umsetzungsplan existieren muss, der den terminierten Weg zur kompletten Erfüllung aufzeigt. Im zweiten Schritt muss nachgewiesen werden, dass man sich entsprechend des Plans im Umsetzungsprojekt befindet, um vor negativen Konsequenzen durch nicht komplette Erfüllung freigestellt zu werden.

Definition IT-Sicherheitsbeauftragte

In §45 und §46 werden die Rollen von IT-Sicherheitsbeauftragen definiert. Dies ist positiv, es bleibt aber zu unkonkret. Sinnvoll wäre die konkrete Benennung von Aufgaben und vor allem Rechten. Das verwendete Wort „beteiligen“ ist de facto wertlos.
So droht die Machtlosigkeit der Rolle, vor allem ob der Unklarheit der organisatorischen Aufhängung. Das BSI empfiehlt für IT-Sicherheitsbeauftragte z. B., dass diese nicht dem IT-Verantwortlichen unterstellt werden, da dies einen Zielkonflikt beinhaltet. Eine solche Regelung inkl. der klaren Benennung der Rechte wäre wünschenswert.

Unscharfe Begrifflichkeiten

- *Management von Anlagen*
  Bereits jetzt führt die „Eindeutschung“ des englischen Begriffs „Asset Management“ zu „Management von Anlagen“ zu Verwirrung, da ja parallel von „Kritischen Anlagen“ gesprochen wird und sich so Unklarheiten ob des Betrachtungsgegenstandes ergeben. Der verwendete deutsche Begriff ist ungebräuchlich, der englische Begriff „Asset Management“ daher zu präferieren.
- *Managed Service Provider*
  Eine weitere begriffliche Unschärfe führt zur Verunsicherung gerade im Maschinenbau. Die Definition der „Managed Service Provider“ (MSP) ist problematisch. Monitoring Services und Remote Access sind Standarddienstleistungen eines Großteils der Hersteller. Nach der aktuellen Begriffsbestimmung müsste ein Großteil des deutschen Maschinenbaus als besonders wichtige Einrichtungen eingestuft werden.
  Das gleiche Problem tritt auf, wenn eine Tochtergesellschaft eines Konzerns den anderen Konzerntöchtern IT-Dienstleistungen anbietet (und zwar ausschließlich). Nach aktueller Lesart wären sie damit MSP im Sinne des Gesetzes. Dies erscheint nicht sinnvoll, es sollte eine Klarstellung geben, dass von Ausfällen betroffene Kunden außerhalb der Konzernsphäre liegen.

Geschäftsführungsverantwortlichkeit

Die Formulierung des §38 im 3. Referentenentwurf war passender als die aktuelle. Aktuell wird gefordert, dass die Geschäftsführung die Maßnahmen umsetzt. In der Praxis (und früher auch passender formuliert) lässt die Geschäftsführung Maßnahmen umsetzen, lässt die Umsetzung überwachen und verantwortet diese.

Angesichts des bereits bestehenden Haftungsregimes ist es zielführend, dass das NIS2UmsuCG als Auffangregelung gilt, sofern keine entsprechende Managerhaftung vorgesehen ist.

Untersagung kritischer Komponenten (ehemalig §9b)

Losgelöst vom Inhalt wäre hier im Vorfeld eine Evaluation des bisherigen Procederes notwendig gewesen. Das bisherige und nun unverändert übernommene Verfahren war schon für einen Sektor sehr zeitfressend und aufwändig, bei vermuteter Verzehnfachung wird dies noch schlimmer und impraktikabel.

Konformitätserklärung §53

Dazu gibt es kein Pendant in NIS2. Der Mehrwert hier erschließt sich mir spätestens nach Verabschiedung des Cyber Resillience Acts nicht und es besteht die Gefahr nationaler Alleingänge, die bei der Industrie auf keinerlei Interesse stoßen.

4. Zur Person

Timo Kob ist Gründer und Eigentümer der HiSolutions AG, einem Beratungshaus für Cybersecurity mit derzeit rund 400 Mitarbeitern.

HiSolutions hält nicht nur die Rahmenverträge des BSI für

- die Erstellung von Sicherheitskonzepten der unmittelbaren Bundesverwaltung und
- die Durchführung von vom BSI angeordneten KRITIS-Tiefenprüfungen in den Unternehmen,

sondern auch des Landes Berlin für

- die Erstellung von Sicherheitskonzepten des Landes und der Bezirke

und kennt u. a. aus diesen Projekten den Sicherheitsstatus sowohl auf privatwirtschaftlicher Seite als auch aus Bund, Ländern und Kommunen.

Er selbst ist vom BSI akkreditierter IT-Grundschutzauditor und leitet darüber hinaus eines von zwei „CertLabs“ des BSI, in denen die Prüfung und Abnahme aller Grundschutzzertifizierungen durchgeführt werden.

Er ist Professor für Cybersecurity und Wirtschaftsschutz an der FH Campus Wien.

Er leitet die Bundesfachkommission Cybersecurity des Wirtschaftsrates der CDU, sitzt im Hauptvorstand sowie im Vorstand des Arbeitskreises Sicherheitspolitik des Bitkom und ist als Vertreter des VDMA im Vorstand des Arbeitskreises Cybersecurity des BDI.

Aus diesen Rollen heraus hat er an den jeweiligen Stellungnahmen der Verbände zum NIS2UmsuCG mitgearbeitet, deren Ergebnisse auch mit in diese Stellungnahme eingeflossen sind.

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
20(4)523 B

schwarz digits

Schwarz Digits KG
Stiftsbergstraße 1 | 74172 Neckarsulm

Deutscher Bundestag
Ausschuss für Inneres und Heimat
Herrn Prof. Dr. Lars Castellucci
Platz der Republik 1
11011 Berlin

Per E-Mail an innenausschuss@bundestag.de

Boris Eisengräber
Leiter Cybersecurity
Telefon 07132 30-456135
boris.eisengraeber@mail.schwarz

Neckarsulm, 30.10.2024

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

Sehr geehrter Herr Abgeordneter,

beiliegende Stellungnahme zu dem oben genannten Gesetzentwurf übersende ich Ihnen mit der Bitte, diese an die Berichterstattenden der Fraktionen und Mitglieder des Ausschusses weiterzuleiten.

Mit freundlichen Grüßen

Boris Eisengräber
Leiter Cybersecurity
Schwarz Digits

Stellungnahme

von Boris Eisengräber, Leiter Cybersecurity, Schwarz Digits

zum Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung
Drucksache 20/13184

1. Grundsätzliche Anmerkungen

Ziel der NIS2-Richtlinie ist die Einführung verbindlicher Maßnahmen für Verwaltung und Wirtschaft, mit denen in der gesamten Europäischen Union ein hohes gemeinsames Cybersicherheitsniveau sichergestellt werden soll. Dies trägt zur Stärkung der europaweiten Harmonisierung der Cybersicherheitsregulierung bei – ein richtiger Schritt im Kontext der angespannten Bedrohungslage im Cyberraum. Auch kritische Infrastrukturen, die öffentliche Hand und Politik stehen immer stärker im Zentrum von Cyberangriffen. Dies stellt eine bedeutsame Bedrohung des Gemeinwesens dar. Auf Grund der Abhängigkeit einzelner Unternehmen von funktionierenden Lieferketten, Infrastruktur und Behörden, ist die übergreifende Definition und Durchsetzung eines Mindestsicherheitsniveaus begrüßenswert und notwendig.

NIS2 umfasst gegenüber der NIS1 sinnvolle Verbesserungen. Hierbei sind im Besonderen hervorzuheben: Die Konkretisierung der geforderten Absicherungsmaßnahmen sowie Fokussierung auf ein aktives Management zur Behandlung von Cyberrisiken.

Die geforderten Absicherungsmaßnahmen sind angemessen und folgen Best-Practices, welche im Wesentlichen von Unternehmen und Organisationen ohnehin aus Eigeninteresse zum Schutz gegen Cyberbedrohungen, getroffen werden sollten.

2. Kongruenz mit dem KRITIS-Dachgesetz

Das NIS2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG) und das KRITIS-Dachgesetz sollten stärker aufeinander abgestimmt werden (insb. bei den definierten Sektoren und zuständigen Behörden). Sowohl das NIS2UmsuCG wie auch das KRITIS-Dachgesetz zielen auf den Schutz kritischer Infrastrukturen ab. Im Besonderen bei hybriden Angriffsszenarien ist eine klare Abgrenzung des Schutzes des physischen Raums und des Cyberraums oft nicht eindeutig möglich. Insofern ist auch auf gesetzlicher Ebene ein ganzheitliches, aufeinander abgestimmtes Schutzkonzept erforderlich. Unternehmen, die von beiden gesetzlichen Regelwerken betroffen sind, können vor verschiedenen Herausforderungen stehen, wie z.B. doppelte Meldepflichten an unterschiedliche Behörden (aktuell Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK), Bundesamt für Sicherheit in der Informationstechnik (BSI) und andere sektorale Aufsichtsbehörden). Während die NIS2-Richtlinie auf eine Harmonisierung auf EU-Ebene abzielt, könnten parallele Regelungen wie das KRITIS-Dachgesetz zu Lücken oder Überschneidungen führen. Dies kann für unnötige Bürokratie, Effizienzverluste und Unsicherheiten bei den betroffenen Unternehmen sorgen. Es gilt daher mit dem NIS2UmsuCG und dem KRITIS-Dachgesetz ein einheitliches Verständnis darüber zu entwickeln, wie physische Sicherheit und Cybersicherheit gemeinsam umgesetzt werden können. Dies umfasst auch die abgestimmte Operationalisierung von Anforderungen aus beiden Gesetzen wie z.B. Risikomanagementmaßnahmen, Bewältigung von Sicherheitsvorfällen oder Notfall- und Krisenmanagement.

Die in § 32 definierte gemeinsame Meldestelle für das BSI sowie das BBK ist hierbei eine positive Entwicklung.

3. Europaweit einheitliche Nachweis-, Melde- und Registrierungspflichten

Die definierten Nachweis-, Melde- und Registrierungspflichten können zu einer besseren präventiven Absicherung sowie einer besseren Reaktion auf Cyberangriffe auf nationaler und europäischer Ebene sowie in einzelnen Organisationen führen. Jedoch können unterschiedliche Umsetzungen der jeweiligen Mitgliedsstaaten bei den geforderten Nachweis-, Melde- und Registrierungspflichten für EU-weit agierende Unternehmen eine Herausforderung darstellen und effektive Reaktionen auf Cyberangriffe erschweren.

So muss ein Sicherheitsvorfall, der in mehreren Mitgliedstaaten Auswirkungen auf die Erbringung der kritischen Dienstleistung haben kann, jeweils an die jeweiligen Computer Security Incident Response Teams (CSIRT) der Mitgliedsstaaten gemeldet werden. Hier wären eine weitere Konkretisierung und Vereinfachung der Meldepflichten auf EU-Ebene begrüßenswert.

Gleiches gilt für in Teilen unterschiedliche Anforderungen der Mitgliedsstaaten hinsichtlich der Nachweispflichten. Dies kann zu Mehrfachprüfungen der gleichen Infrastruktur bei EU-weit agierenden Unternehmen führen.

Ein möglicher Lösungsansatz ist Nachweis-, Melde- und Registrierungspflichten auf den Mitgliedsstaat zu beschränken, in dem die jeweilige IT-Infrastruktur maßgeblich (physisch und damit lokal vor Ort in einem Mitgliedsstaat) betrieben wird.

4. Überprüfung Risikomanagementmaßnahmen

Neben dem Fokus auf reaktive Risikomanagementmaßnahmen, wie die Erkennung und Bewältigung von Sicherheitsvorfällen oder Krisenreaktion, ist auch die Berücksichtigung von präventiven Sicherheitsmaßnahmen wie z.B. die Identifikation von durch Angreifer ausnutzbare Sicherheitslücken oder Fehlkonfigurationen von IT-Systemen wichtig und hervorzuheben, um erfolgreiche Angriffe bestmöglich zu vermeiden. Hierbei ist im Besonderen bei weiteren Konkretisierungen wie z.B. im Rahmen von Durchführungsverordnungen der EU zu beachten, dass die Technologieoffenheit gewahrt bleibt und Unternehmen weiterhin die Möglichkeit haben die identifizierten Risiken auf die jeweilige Situation angepasst nach aktuellen Best Practices zu mitigieren.

Auf Grund der stetigen Veränderung des Angreiferverhaltens im Cyberraum, der technischen Innovationen im Kontext der Digitalisierung sowie der Automatisierung von Verteidigungsmaßnahmen, sollten die konkreten Anforderungen an nicht-technische Maßnahmen und eingesetzte Technologien von den Gesetzgebungsprozessen entkoppelt werden. Darüber hinaus sollten die technischen Anforderungen und Maßnahmen regelmäßig überprüft und bei Bedarf angepasst werden.

5. Wichtigkeit der Rolle des Bundesamtes für Sicherheit in der Informationstechnik (BSI)

Während unter der vorherigen Regulierung eine mittlere vierstellige Anzahl an Unternehmen von Cybersicherheitsmindestanforderungen und Meldepflichten betroffen waren, erhöht sich diese Anzahl auf rund 29.500 Unternehmen, bei gleichzeitiger Kürzung des BSI-Haushalts für 2025[1]. Das BSI ist zentrale Anlaufstelle aller betroffenen oder potenziell betroffenen Unternehmen in Bezug auf das NIS2UmsuCG und der Umsetzung der darin enthaltenen Risikomanagementmaßnahmen, Registrierungs- und Meldepflichten. Durch die Bereitstellung geeigneter Tools, wie der NIS-2-Betroffenheitsprüfung, das Erstellen von Orientierungshilfen oder FAQs, das Versenden von IT-Tageslageberichten oder die Teilnahme an Themenarbeitskreisen sowie Branchenarbeitskreisen, leistet das BSI einen wesentlichen Beitrag, um in gemeinsamer Zusammenarbeit das Cybersicherheitsniveau auf nationaler, aber auch internationaler Ebene nachhaltig zu erhöhen. Eine eingeschränkte Arbeits-/Leistungsfähigkeit des BSI könnte der effektiven Umsetzung des NIS2UmsuCG bei den betroffenen Unternehmen entgegenstehen.

Meldungen der von NIS2UmsuCG betroffenen Unternehmen entfalten nur dann die gewünschte Wirkung, wenn diese zeitnah und fachgerecht durch das BSI (CSIRT) verarbeitet werden und abgeleitete Informationen und Berichte an die Unternehmen weitergegeben werden.

Die gute Zusammenarbeit zwischen Unternehmen und dem BSI ist ein wesentlicher Erfolgsfaktor für die Verbesserung der Cybersicherheit in Deutschland und sollte daher weiter gestärkt und ausgebaut werden.

6. Cybersicherheit ist eine gesamtgesellschaftliche Aufgabe

Ein effektives Cybersicherheitsniveau kann nicht allein durch das BSI oder die jeweiligen Sicherheitsfunktionen in Unternehmen gewährleistet werden. Vielmehr ist dies eine gesamtgesellschaftliche Aufgabe.

Das NIS2UmsuCG erweitert den Anwendungsbereich auf zahlreiche neue unter die Regulierung fallende Unternehmen und wird große Teile der deutschen Wirtschaft betreffen.

Der Ausschluss staatlicher Stellen und Behörden im NIS2UmsuCG ist der falsche Weg und schwächt die staatliche Vorbildfunktion und das einheitliche Cybersicherheitsniveau.

---

[1] BMI-Pressemitteilung 24.07.2024 (Wirtschaft und Staat vor Cyberattacken schützen: Bundesregierung beschließt umfassende Änderung des IT-Sicherheitsrechts) und Entwurf eines Gesetzes über die Feststellung des Bundeshaushaltsplans für das Haushaltsjahr 2025 (Drucksache 20/12400)

Zur Verbesserung der Cybersicherheit im öffentlichen Sektor gehört neben der Stärkung des BSI und weiterer Sicherheitsfunktionen auch die Modernisierung der IT-Infrastruktur nach Stand der Technik und der Bereitstellung des hierfür erforderlichen Budgets bei Bund, Ländern und Kommunen.

Die im Gesetzesentwurf erwähnten geänderten wirtschaftspolitischen und geopolitischen Rahmenbedingungen machen deutlich, dass die Etablierung eines angemessenen Cybersicherheitsniveaus in Europa auch die Stärkung der europäischen Souveränität im Kontext der eingesetzten IT-Infrastruktur umfassen muss.

Schwarz Digits KG
Stiftsbergstraße 1 | 74172 Neckarsulm | Telefon: +49 7132 30-7000
Kommanditgesellschaft | Sitz: Neckarsulm | Registergericht: Stuttgart, HRA 737212 | USt-IdNr.: DE335467503

Vertretungsberechtigte Komplementärin:
Ny-Stiftung | Sitz: Dresden | Landesdirektion Sachsen, AZ 20-2245/589

Claudia Plattner – Präsidentin des BSI

Stellungnahme zur öffentlichen Anhörung des Innenausschusses des Deutschen Bundestages am 4. November 2024

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
20(4)523 C

Der Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz) ist aus meiner fachlichen Sicht grundsätzlich dazu geeignet, das Cybersicherheitsniveau in Deutschland anzuheben. Gleichwohl wäre im Sinne gesamtstaatlicher Cybersicherheit die Aufnahme von Kommunen wünschenswert und es besteht meines Erachtens erheblicher Nachbesserungsbedarf zur Stärkung des BSI als zentrale Stelle für Cybersicherheit, der nachfolgend dargelegt wird.

Übersicht

1 CISO Bund fest bei BSI verankern

Ein starker CISO Bund sollte beim BSI angesiedelt werden, weil dieses schon die notwendigen Fach- und Umsetzungskompetenzen besitzt und – verknüpft mit der unabhängigeren Stellung des BSI – als neutrale Stelle für Cybersicherheit wirkt. Weiterhin würde eine Verortung des CISO Bund beim BMI absehbar zu operativen Reibungsverlusten führen, beispielsweise wenn Behörden Sicherheitsvorgaben des BSI vor einer Umsetzung erst mit dem CISO Bund rückkoppeln. Wenn der CISO Bund beim BSI platziert wird, kann ein effektives prozessuales Verschränken zwischen den Befugnissen des BSI bezüglich der Cybersicherheit der Bundesverwaltung im Rahmen der NIS2-Richtlinie und dem operativen Wirken des CISO Bund sichergestellt werden. Dies wäre ein deutlicher Gewinn für die Informationssicherheit der Bundesverwaltung.

Aus diesen Gründen sollte die Rolle des CISO Bund explizit als zusätzliche Aufgabe des BSI im BSIG aufgenommen werden und dort mit einer klaren Zweckbestimmung versehen werden. Damit ein CISO Bund effektiv arbeiten kann und tatsächlich Wirkung entfaltet, ist es unabdingbar, dass die Position mit den erforderlichen Befugnissen ausgestattet wird, um die dazugehörigen Aufgaben zielgerichtet zu erfüllen. Das BSI verfügt bereits über entsprechende Durchsetzungsbefugnisse – es müsste daher nur festgelegt werden, dass diese ebenso dem CISO Bund zur Verfügung stehen, wenn die Rolle beim BSI verankert wird. Aus fachlicher Sicht des BSI sollten nachfolgende Änderungen umgesetzt werden:

a) Aufnahme des CISO Bund als zusätzliche Aufgabe des BSI
   Indem die Position unmittelbar hinter den Aufgaben des BSI in einem neuen § 3a aufgenommen wird, wird durch die Gesetzessystematik deutlich, dass es sich bei der Rolle um eine zusätzliche und wichtige Aufgabe des BSI handelt.

   ⇨ *Empfehlung für neuen § 3a BSIG „Die oder der Bundesbeauftragte für Informationssicherheit“:*

   „(1) Die Leitung des Bundesamtes nimmt die Aufgaben der oder des Bundesbeauftragten für Informationssicherheit (Bundesbeauftragte) wahr.

   Sie oder er muss über die für die Erfüllung ihrer oder seiner Aufgaben und Ausübung ihrer oder seiner Befugnisse erforderliche Qualifikation, Erfahrung und Sachkunde insbesondere im Bereich der Informationssicherheit verfügen.

   (2) Die oder der Bundesbeauftragte wirkt gemeinsam mit dem Beauftragten der Bundesregierung für Informationstechnik auf ein angemessenes Verhältnis zwischen dem Einsatz von Informationstechnik und Informationssicherheit hin.

   (3) Die oder der Bundesbeauftragte wird bei allen Gesetzes-, Verordnungs- und sonstigen wichtigen Vorhaben beteiligt soweit sie Fragen der Informationssicherheit berühren.“

b) Festlegung der erforderlichen Zweckbestimmung der Rolle CISO Bund
Die Position „Bundesbeauftragte“ erfordert eine grundsätzliche Zweckbestimmung der Rolle. Für die Rolle des CISO Bund ist dies aus hiesiger Sicht die Koordinierung des Informationssicherheitsmanagements des Bundes.

⇨ *Empfehlung für neuen § 3b BSIG „Aufgaben der oder des Bundesbeauftragten“:*

„Die oder der Bundesbeauftragte koordiniert das Informationssicherheitsmanagement des Bundes. Im Benehmen mit den obersten Bundesbehörden entwickelt die oder der Bundesbeauftragte Programme zur Gewährleistung der Informationssicherheit des Bundes und schreibt diese fort. Sie oder er unterrichtet kalenderjährlich jeweils bis zum 30. Juni den Haushaltsausschuss des Deutschen Bundestages über den Umsetzungsstand der Programme.“

c) Festlegung der erforderlichen Befugnisse für zielgerichtete Aufgabenwahrnehmung
Zur zielgerichteten Aufgabenwahrnehmung kann die Rolle des CISO Bund ihre Wirkung nur entfalten, wenn damit die notwendigen Durchsetzungsbefugnisse in Sachen IT-Sicherheit verbunden werden.

⇨ *Empfehlung für neuen § 3c BSIG „Befugnisse der oder des Bundesbeauftragten“:*

„(1) Der oder die Bundesbeauftragte beaufsichtigt die Umsetzung der Programme zur Gewährleistung der Informationssicherheit des Bundes durch die Befugnisse des Bundesamtes nach diesem Gesetz.

(2) Zur Wahrnehmung ihrer oder seiner Aufgaben hat die oder der Bundesbeauftragte ein direktes Vortragsrecht vor dem Ausschuss für Inneres und Heimat und dem Haushaltsausschuss des Deutschen Bundestages des Deutschen Bundestages zu allen Themen der Informationssicherheit des Bundes.“

2 Unabhängigere Rolle des BSI etablieren

Mit der im Koalitionsvertrag vereinbarten unabhängigeren Aufstellung des BSI wird der bestehende Interessenskonflikt zwischen öffentlicher Sicherheit und Informationssicherheit im Geschäftsbereich des BMI entschärft und die fachliche Unabhängigkeit des BSI klargestellt. Mit Aufstellung des BSI als selbstständige Bundesoberbehörde, würde die Rolle des BSI bereits unabhängiger, ohne das Bundesamt aus dem Geschäftsbereich des BMI herauszulösen. Zudem könnte das BMI in einem neuen Aufsichtskonzept die Grundlinien der Fachaufsicht für das BSI festlegen und dort bspw. die gemeinsame Erstellung eines Jahresarbeitsprogramms für das BSI vorsehen. Um die Position des BSI als neutrale und unabhängige Beratungsinstanz für die Bundesressorts sicherzustellen, sollte die Berichtspflicht des BSI an das BMI bei der Zusammenarbeit mit anderen Ressorts entfallen. Aus fachlicher Sicht des BSI sollten hierfür nachfolgende Änderungen umgesetzt werden:

a) Aufstellung des BSI als selbstständige Bundesoberbehörde
Mittels dieser Statusänderung würde die Rolle des BSI bereits unabhängiger gestaltet und zugleich ein hoher Grad an demokratischer Legitimation erhalten bleiben.

⇨ *Empfehlung zur Änderung von § 1 Satz 1 BSIG:*

„Das Bundesamt für Sicherheit in der Informationstechnik (Bundesamt) ist eine selbständige Bundesoberbehörde im Geschäftsbereich des Bundesministeriums des Innern und für Heimat."

b) Fixierung der wissenschaftlich-technischen Arbeitsgrundlage des BSI
Die Arbeit des BSI auf Grundlage rein wissenschaftlich-technischer Erkenntnisse sollte explizit im BSIG festgeschrieben werden, um die fachlich unabhängige Aufgabenwahrnehmung des BSI zu betonen und dadurch die Vertrauenswürdigkeit des BSI zu stärken.

⇨ *Empfehlung zur Änderung von § 1 Satz 3 BSIG:*

„Das Bundesamt führt seine Aufgaben fachlich unabhängig auf Grundlage wissenschaftlich-technischer Erkenntnisse durch."

c) Gemeinsame Erstellung eines Jahresarbeitsprogramms des BSI zwischen BMI und BSI
Im Rahmen einer neu gestalteten Fachaufsicht könnte das BMI in einem Aufsichtskonzept die Grundlinien der Fachaufsicht über das BSI festlegen und dort die Erstellung eines Jahresarbeitsprogramms für das BSI gemeinsam mit dem BSI vorsehen. Um eine angemessene Transparenz gegenüber dem Bundestag zu gewährleisten, könnte das BMI alle zwei Jahre das Parlament über die Aufsichtspraxis und Einzelweisungen an das BSI unterrichten.

⇨ *Empfehlung für neuen § 1 Satz 4 BSIG:*

„Das Bundesministerium des Innern und für Heimat erstellt Grundlinien der Aufsicht über das Bundesamt in einem Aufsichtskonzept und unterrichtet alle zwei Jahre den Deutschen Bundestag über die Aufsichtspraxis und Einzelweisungen an das Bundesamt."

d) Wegfall der Berichtspflicht des BSI an BMI bei der Zusammenarbeit mit anderen Ressorts
Mit Umsetzung des nachstehenden Vorschlags wäre es dem BSI möglich, andere Ressorts neutral und unabhängig zu beraten. Die bisherige negative Sonderstellung des BSI in der GGO ist sachlich nicht gerechtfertigt und im Hinblick auf die Funktion als zentraler Kompetenzträger für alle Stellen des Bundes in Sachen der IT-Sicherheit auch kontraproduktiv.

⇨ *Empfehlung zur Streichung der Nennung des BSI aus § 26 Abs. 1 S. 2 GGO*

3 Operative Abwehrfähigkeiten des BSI weiter stärken

Stärkung der Cyberabwehrfähigkeiten gegen Botnetze

Das BSI setzt seit mehreren Jahren Maßnahmen zur Abwehr von Botnetzen um, darunter auch die Umleitung von Domainnamen durch Internetprovider. Gleichwohl nutzen Botnetze zunehmend neue Techniken wie DNS over HTTPS, bei denen eine vom BSI angeordnete Umleitung von Domainnamen durch Provider keinen flächendeckenden Schutz bietet, da viele Nutzende auch andere zulässige Möglichkeiten zur Auflösung von Domainnamen verwenden. Dies liegt darin begründet, dass nur die Kunden großer deutscher Internetanbieter (>100.000 Kunden) geschützt werden, die auch tatsächlich den vorgegebenen DNS-Dienst des Anbieters nutzen. Die angeordnete Domain bleibt weiterhin für alle anderen Internetnutzer international aktiv und weiterhin erreichbar. Nur durch eine Dekonnektierung der Domain auf Ebene der Nameserver kann ein vollständiger Schutz für alle Nutzer umgesetzt werden. Damit das BSI auch weiterhin in der Lage ist, Botnetze zu analysieren und zu entschärfen, ist eine Ausdehnung der bisherigen Anordnungsbefugnis auf Domainregistare dringend geboten, um die operativen Handlungsmöglichkeiten des BSI an die technischen Entwicklungen anzupassen. Aus fachlicher Sicht des BSI sollte hierfür nachfolgende Änderung umgesetzt werden:

- ⇨ *Empfehlung zur Einführung eines neuen § 17a BSIG „Anordnungen des Bundesamtes gegenüber Top Level Domain Name Registries und Registraren“:*

  „(1) Zur Abwehr konkreter erheblicher Gefahren für die in Absatz 2 genannten Schutzgüter kann das Bundesamt gegenüber Top Level Domain Name Registries oder Registraren im Sinne dieses Gesetzes anordnen, dass sie

  a) die Nameserver Einträge einer vom Bundesamt benannten Domain ändern, neue Einträge hinzufügen oder die Domain auf Ebene der Nameserver dekonnektieren oder
  b) dem Bundesamt die Inhaberschaft an einer bestimmten Domain übertragen,

  sofern und soweit der Diensteanbieter dazu technisch in der Lage ist und es ihm wirtschaftlich zumutbar ist. Widerspruch und Anfechtungsklage gegen die Anordnungen nach Satz 1 haben keine aufschiebende Wirkung. Im Fall des Absatz 1 Satz 1 Nummer 2 benennt das Bundesamt die zur Übertragung der Inhaberschaft notwendigen Ansprechpartner.

  (2) Schutzgüter gemäß Absatz 1 Satz 1 sind die Verfügbarkeit, Integrität oder Vertraulichkeit

  a) der Kommunikationstechnik des Bundes, einer Kritischen Einrichtung oder einer besonders wichtigen Einrichtung oder einer wichtigen Einrichtung,
  b) von Informations- oder Kommunikationsdiensten oder

c) von Informationen, sofern deren Verfügbarkeit, Unversehrtheit oder Vertraulichkeit durch unerlaubte Zugriffe auf eine erhebliche Anzahl von telekommunikations- oder informationstechnischen Systemen von Nutzern eingeschränkt wird.

(3) Ordnet das Bundesamt eine Maßnahme nach Absatz 1 Satz 1 lit. a) an, so kann es gegenüber einer Top Level Domain Name Registry oder einem Registrar auch anordnen, die an eine bestimmte Domain gerichteten Nameserveranfragen an einen vom Bundesamt benannten Nameserver umzuleiten.

(4) Das Bundesamt darf Daten, die von einer Top Level Domain Name Registry oder einem Registrar nach Absatz 1 Satz 1 lit. a und Absatz 3 umgeleitet wurden, verarbeiten, um Informationen über Schadprogramme oder andere Sicherheitsrisiken in informationstechnischen Systemen zu erlangen. Die übermittelten Daten dürfen durch das Bundesamt so lange gespeichert werden, wie dies für die Erfüllung des in Satz 1 genannten Zwecks erforderlich ist, längstens jedoch für drei Monate. § 5 Absatz 7 Satz 2 bis 8 gilt entsprechend. Das Bundesamt unterrichtet die Bundesbeauftragte oder den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit jeweils bis zum 30. Juni des Folgejahres über die Gesamtzahl der angeordneten Nameserverumleitungen.

(5) Die nach Absatz 1 Satz 1 lit. b) übertragenen Inhaberschaften müssen vom Bundesamt aufgegeben werden, wenn feststeht, dass

a) von den Domains keine Gefahren nach Absatz 1 Satz 1 mehr ausgehen, und
b) über die Inhaberschaft an den Domains keine Informationen über Schadprogramme oder andere Sicherheitsrisiken in informationstechnischen Systemen mehr zu erlangen sind.

In diesem Fall wird das Bundesamt die Inhaberschaften durch Veranlassung der Löschung der Domains bei der zuständigen Top Level Domain Name Registry oder dem zuständigen Registrar veranlassen."

Erweiterte Befugnis zur Messung der Resilienz deutscher IT-Systeme gegenüber aktuellen Schwachstellen

Derzeit darf das BSI gemäß § 7b BSIG (nach Regierungsentwurf zukünftig § 15 BSIG) Resilienz-Messungen bei öffentlich erreichbaren IT-Systemen nur in einem sehr eingeschränkten Bereich durchführen. Bisher sind davon lediglich die Einrichtungen des Bundes, Kritische Infrastrukturen, Digitale Dienste (z.B. Online-Marktplätze,-Suchmaschinen und Cloud-Computing-Dienste) sowie Unternehmen im besonderen öffentlichen Interesse umfasst.

Mit einer Erweiterung der Befugnisse, solche Resilienz-Messungen hinsichtlich der Verwundbarkeit aufgrund öffentlich bekannter Schwachstellen für alle im deutschen IP-Raum erreichbaren IT-Systeme durchzuführen, würde ein signifikanter Mehrwert für die IT-Sicherheit

deutschlandweit generiert. Ausschließliches Ziel dieser Messungen ist die Warnung der Betroffenen, damit diese möglichst zeitnah Schutzmaßnahmen ergreifen können. Dem BSI wäre es dann möglich, in einem transparenten Verfahren alle Betroffenen schnell und effektiv über die Verwundbarkeit ihrer IT-Systeme zu informieren. Dies kann über die Möglichkeit für das BSI sichergestellt werden, Provider entsprechend zur Information ihrer Kundinnen und Kunden anzuweisen.

Die Befugniserweiterung dient ausdrücklich nicht zur heimlichen Suche nach Schwachstellen in deutschen IT-Systemen, um diese auszunutzen. Das BSI wird also nicht zu einer „Hackerbehörde". Im Gegenteil bleibt mit der Befugniserweiterung auch die unverzügliche Benachrichtigungspflicht bestehen (§ 15 Abs. 2 BISG-E), die für maximale Transparenz sorgt: Das BSI sucht nach Schwachstellen, um die Betroffenen zeitnah über ihre Verwundbarkeit zu informieren, damit diese ihre Systeme schnellstmöglich sichern können. Es handelt es sich somit um eine Befugnis des Bundesamtes mit strenger Zweckbindung. Die entsprechenden Detektionsmaßnahmen dürfen nur zur Aufgabenerfüllung genutzt werden.

Insbesondere bei weit verbreiteten kritischen Schwachstellen, z.B. in Microsoft Exchange Servern, wäre es dem BSI mit dieser erweiterten Befugnis möglich, binnen kürzester Zeit, verwundbare Systeme zu identifizieren und die Betreiber mittels schneller Warnung zum Schließen der Schwachstellen zu animieren. Aktuell wird die Betroffenheit von den Betreibern zu oft erst nach erfolgreichen Angriffen bekannt. Für die IT-Sicherheit in Deutschland würde diese Befugniserweiterung daher einen deutlichen Gewinn bei minimalem zusätzlichen Ressourcenaufwand bedeuten. Ergänzend dazu ließe sich mit den Gefährdungsübersichten aus den erweiterten Resilienz-Messungen das gesamtdeutsche Cybersicherheits-Lagebild noch weiter schärfen. Aus fachlicher Sicht des BSI sollten die Befugniserweiterung nachfolgende Änderung umgesetzt werden:

- ⇨ *Empfehlung zur Anpassung des § 15 Abs. 1 BSIG-E (vormals § 7b BSIG) zur Erweiterung der Befugnis zur Resilienz-Messung von deutschen IT-Systemen:*

  „(1) 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 der Bundesverwaltung, bei besonders wichtigen Einrichtungen oder bei wichtigen Einrichtungen~~ Abfragen an den Schnittstellen öffentlich erreichbarer informationstechnischer Systeme zu öffentlichen Telekommunikationsnetzen durchführen,

  ~~1.~~ um festzustellen, ob diese Schnittstellen unzureichend geschützt und dadurch in ihrer Sicherheit oder Funktionsfähigkeit gefährdet sein können~~, oder~~

  ~~2. wenn die entsprechenden Einrichtungen der Bundesverwaltung, besonders wichtige oder wichtige Einrichtungen darum ersuchen~~.
  Die dadurch gewonnenen Erkenntnisse dürfen nur zum Zweck der Information nach Absatz 2 verwendet werden. Erlangt das Bundesamt dabei Informationen, die durch Artikel 10 des Grundgesetzes geschützt sind, sind diese unverzüglich zu löschen."

4 Wirksamkeit des BSI verbessern

Zielführende Anpassung von Einvernehmenserfordernissen im Bereich KRITIS

Der aktuelle Regierungsentwurf sieht für das BSI deutlich mehr Einvernehmenserfordernisse beim Aufsichtshandeln vor, als dies für die BNetzA der Fall ist. Es sollte sichergestellt werden, dass für ein gleichmäßiges Wahrnehmen der behördlichen Aufsicht die Einvernehmens- und Benehmenserfordernisse für BSI und BNetzA symmetrisch ausgestaltet werden. Insbesondere bei der einfachen Durchsetzung formaler gesetzlicher Pflichten bezüglich der Registrierung von Unternehmen nach § 33 Abs. 3 BSIG-E sollte auf ein Einvernehmen des BSI mit den jeweils zuständigen Aufsichtsbehörden verzichtet werden, um unnötigen bürokratischen Mehraufwand zu vermeiden. Auch bei der Herausgabe von Informationen durch Unternehmen im Zuge eines erheblichen Sicherheitsvorfalls (§ 40 Abs. 5 BSIG-E) sollte unbedingt auf das derzeit im Entwurf vorgesehene Einvernehmenserfordernis für das BSI verzichtet werden. Während eines solchen Sicherheitsvorfalls hat die zeitnahe Bewältigung oberste Priorität. Die Herstellung des Einvernehmens durch das BSI mit den jeweils zuständigen Aufsichtsbehörden des Bundes nur für die Herausgabe von notwendigen Informationen steht dem diametral entgegen.

Dagegen ist die Einvernehmensregelung bei einer Anordnung zur Mängelabstellung sinnvoll, weil dadurch die Aufsichtsbehörde inhaltlich mitbewerten kann. Zudem sollte auch der Katalog von IT-Sicherheitsanforderungen für Betreiber von Energieanlangen und –versorgungsnetzen nur im Einvernehmen mit dem BSI durch die BNetzA festgelegt und aktualisiert werden, anstatt wie bisher im Regierungsentwurf vorgesehen, lediglich im Benehmen (§ 5c Abs. 1,2 EnWG-E). Dies entspricht zugleich auch der bestehenden Gesetzeslage im Bereich der Telekommunikation (vgl. § 167 Abs. 1 TKG). Eine unterschiedliche Behandlung der Sektoren ist nicht erklärbar und würde zu einer auch verfassungsrechtlich problematischen, divergierenden Ausgestaltung von IT-Sicherheitsanforderungen zwischen diesen führen. Aus fachlicher Sicht des BSI sollten demzufolge nachfolgende Änderungen umgesetzt werden:

- ⇨ *Empfehlung zur Anpassung von § 33 Abs. 3 BSIG-E bezüglich der Registrierungspflicht von Unternehmen:*

  „(3) Die Registrierung von besonders wichtigen Einrichtungen und wichtigen Einrichtungen und Domain-Name-Registry-Diensteanbietern kann das Bundesamt ~~im Einvernehmen mit den jeweils zuständigen Aufsichtsbehörden~~ auch selbst vornehmen, wenn ihre Pflicht zur Registrierung nicht erfüllt wird.“

- ⇨ *Empfehlung zur Anpassung von § 40 Abs. 5 Satz 1 BSIG-E bezüglich der Herausgabe von Informationen zur laufenden Vorfallsbewältigung:*

  „(5) Während eines erheblichen Sicherheitsvorfalls gemäß § 32 Absatz 1 kann das Bundesamt ~~im Einvernehmen mit der jeweils zuständigen Aufsichtsbehörde des Bundes~~ von den betroffenen Betreibern kritischer Anlagen die Herausgabe der zur

Bewältigung der Störung notwendigen Informationen einschließlich personenbezogener Daten verlangen."

⇨ *Empfehlung zur Anpassung von § 5c Abs. 1, 2 EnWG-E zur Ergänzung des Einvernehmens des BSI hinsichtlich des IT-Sicherheitskatalogs für Energieversorgungsnetze und Energieanlagen:*

„(1) (...) Die Bundesnetzagentur bestimmt im Einvernehmen ~~Benehmen~~ mit dem Bundesamt für Sicherheit in der Informationstechnik durch Festlegung nach § 29 Absatz 1 in einem Katalog von Sicherheitsanforderungen (IT-Sicherheitskatalog) die Anforderungen an den angemessenen Schutz. Dabei beteiligt die Bundesnetzagentur die Betreiber von Energieversorgungsnetzen und deren Branchenverbände. Die Bundesnetzagentur überprüft den IT-Sicherheitskatalog alle zwei Jahre und aktualisiert ihn bei Bedarf im Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik. (...)

(2) (...) Die Bundesnetzagentur bestimmt im Einvernehmen ~~Benehmen~~ mit dem Bundesamt für Sicherheit in der Informationstechnik durch Festlegung nach § 29 Absatz 1 in einem IT-Sicherheitskatalog die Anforderungen an den angemessenen Schutz. Dabei beteiligt die Bundesnetzagentur die Betreiber nach Satz 1 und deren Branchenverbände. Die Bundesnetzagentur überprüft den IT-Sicherheitskatalog alle zwei Jahre und aktualisiert ihn bei Bedarf im Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik. (...)"

Einschränkungen bei der Fehlersuche im Schadsoftware-Erkennungssystem aufheben

Das BSI betreibt ein Schadsoftware-Erkennungssystem (SES) mit Detektoren, um die Netze des Bundes und die Kommunikation zwischen Behörden zu schützen. Beim Ausfall eines Detektors aufgrund von Datenfehlern läuft dieser bis zur Fehlerbehebung nicht weiter, wodurch die Schutzwirkung des SES gemindert ist. Aktuell besteht jedoch eine Beschränkung bei der anlassbezogenen Auswertung in solchen Ausnahmefällen auf Protokolldaten nach § 5 BSIG und erschwert die schnelle Fehlerbehebung und damit den Einsatz des Detektors im laufenden Betrieb. Denn in der Praxis lassen sich Fehlerquellen nicht über diesen Weg finden, wenn die Fehlerquelle in den Schnittstellendaten liegt. Die bestehende Auswertungsbefugnis des BSI für die Fehlersuche im SES sollte daher zielführend angepasst werden, um die bestehende Lücke bei der Absicherung der Netze des Bundes zu schließen. Aus fachlicher Sicht des BSI sollte hierfür nachfolgende Änderung umgesetzt werden:

⇨ *Empfehlung zur Änderung von § 8 Absatz 3 BSIG-E:*

„(3) Zur Sicherstellung einer fehlerfreien automatisierten Auswertung dürfen Protokolldaten vor ihrer Pseudonymisierung und Speicherung sowie Schnittstellendaten manuell verarbeitet werden.
Liegen Hinweise vor, dass die fehlerfreie automatisierte Auswertung wegen eines erheblichen Fehlers erschwert wird, darf der Personenbezug von Protokolldaten zur

Sicherstellung der fehlerfreien automatisierten Auswertung wiederhergestellt werden, sofern dies im Einzelfall erforderlich ist; Absatz 2 Satz 3 bis 6 gilt entsprechend."

Lagebild weiter vervollständigen durch „Nullmeldungen" der Nachrichtendienste

Für ein vollständiges Lagebild ist es für das BSI relevant zu erfahren, wie häufig sicherheitsrelevante Meldungen vonseiten der Nachrichtendienste bspw. aufgrund von Geheimschutzregelungen oder Vereinbarungen mit Dritten nicht an das BSI weitergegeben werden. Ist diese „Dunkelziffer" dem BSI dagegen nicht vollumfänglich bekannt, reduziert diese Unklarheit die fachlich fundierte Einschätzung der aktuellen Cybersicherheitslage Deutschlands. Der Regierungsentwurf formuliert hierfür richtigerweise eine jährliche verpflichtende Weitergabe der Gesamtzahl solcher Nichtmeldungen anderer Behörden an das BSI – davon ausgenommen sind im Entwurf jedoch der Bundesnachrichtendienst und das Bundesamt für Verfassungsschutz. Seitens des BSI wird von einer kleinen Zahl solcher Nichtmeldungen ausgegangen, sodass durch die zahlenmäßige Erfassung bei BND und BfV kaum Aufwände erzeugt werden dürften. Würde die Zahl der Nichtmeldungen eine erhebliche Größe annehmen, entstünde ein Informationsdefizit im BSI, welches aus Sicht des BSI für die IT-Sicherheit des Bundes nicht akzeptabel wäre. Die Ausnahme für BND und BfV sollte daher entfallen. Aus fachlicher Sicht des BSI sollte hierfür nachfolgende Änderung umgesetzt werden:

⇨ *Empfehlung zur Streichung von § 43 Abs. 5 Satz 5 BSIG-E:*

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

5 Zuständigkeiten im Bereich Energie klar zuordnen

Der Regierungsentwurf führt in Verbindung mit § 5c EnWG zu gedoppelten Zuständigkeiten von BNetzA und BSI für Betreiber im Energiesektor. Zugleich bestände aber aufgrund der derzeitigen Ausgestaltung im Gesetzesentwurf für die betroffenen Unternehmen entweder keine Nachweispflicht über die Absicherung der IT bzw. Teile eines Unternehmens müssten dem BSI und andere Teile der BNetzA entsprechende Nachweise erbringen. Letzteres würde einen erheblichen bürokratischen Mehraufwand für die Betreiber nach sich ziehen. Daher sollte unbedingt eine Zersplitterung der Zuständigkeiten für die IT-Sicherheit in KRITIS-Sektoren vermieden werden. Wie im Koalitionsvertrag vereinbart sollte daher das BSI als zentrale Stelle für Cybersicherheit gestärkt werden und die Zuständigkeit für den Schutz der Cybersicherheit Kritischer Infrastrukturen gebündelt beim BSI verortet werden. Mindestens jedoch sollte die Office-IT in jedem Fall unter BSI-Aufsicht stehen, um eine gleiche Regulierung über alle Sektoren hinweg sicherzustellen und somit die IT-Sicherheit und Versorgungssicherheit zu erhöhen sowie die Anwendbarkeit für Betreiber zu erleichtern. Aus fachlicher Sicht des BSI sollte hierfür nachfolgende Änderung umgesetzt werden:

⇨ *Empfehlung zur Anpassung von § 28 Abs. 4 BSIG-E:*

„(4) Die §§ 30, 31, 32, 35, 36, 38, 39, 61 und 62 sind nicht anzuwenden auf besonders wichtige Einrichtungen und wichtige Einrichtungen, ~~die~~ soweit sie

1. ein öffentliches Telekommunikationsnetz betreiben oder öffentlich zugängliche Telekommunikationsdienste erbringen;
2. Energieversorgungsnetze oder Energieanlagen im Sinne des Energiewirtschaftsgesetzes vom 7. Juli 2005 (BGBl. I S. 1970, 3621), das zuletzt durch Artikel 1 des Gesetzes vom 14. Mai 2024 (BGBl. 2024 I Nr. 161) geändert worden ist, betreiben und den Regelungen des § 5c des Energiewirtschaftsgesetzes unterliegen. (...)“

⇨ *Empfehlung zur Anpassung von § 5c Abs. 3 EnWG-E:*

- Streichen von Nr. 12 in § 5c Abs. 3 Satz 3 EnWG-E

6 Effektives Informationssicherheitsmanagementsystem für den Bund sicherstellen

Damit der CISO Bund nicht ein rein koordinierender „Papiertiger“ wird, muss er ein funktionierendes, effektives Informationssicherheitssystem mit Durchschlagskraft beaufsichtigen. Um dem Anspruch gerecht zu werden, ein hohes Niveau in der Cybersicherheit für die gesamte Bundesverwaltung sicherzustellen, müssen aus hiesiger Sicht drei wesentliche Aspekte erfüllt sein: Entsprechende IT-Sicherheitsvorgaben müssen für die gesamte Bundesverwaltung gelten; die Einrichtungen des Bundes müssen ihre Pflichten eigenverantwortlich umsetzen; die Rechtslage muss es dem BSI ermöglichen, Sicherheitsvorgaben flexibel und zeitnah an die technischen Entwicklungen anzupassen – auch um bürokratischen Mehraufwand für alle Beteiligten zu vermeiden. Aus fachlicher Sicht des BSI sollte hierfür nachfolgende Änderungen umgesetzt werden:

a) Erfassung der gesamten Bundesverwaltung unter Beibehaltung bestehender Ausnahmen
   Um effektiv ein hohes Cybersicherheitsniveau für den Bund gewährleisten zu können, muss auch die Bundesverwaltung zur Einhaltung angemessener IT-Sicherheitsvorgaben verpflichtet werden. Während der Regierungsentwurf die Vorgaben für die Wirtschaft maßgeblich erhöht, werden die Pflichten für den öffentlichen Sektor dagegen reduziert. Damit würden die IT-Sicherheitsvorgaben für den Bund im Vergleich zum aktuellen Stand sogar verringert.
   Der Regierungsentwurf beschränkt die IT-Sicherheitsvorgaben für die Bundesverwaltung auf das Bundeskanzleramt und die Mehrheit der Bundesministerien. Die jeweils nachgeordneten Einrichtungen der Ressorts fallen nicht unter die verpflichtenden Vorgaben. Dies unterminiert das Ziel eines durchgehend hohen IT-Sicherheitsniveaus in der gesamten Bundesverwaltung. Zudem sieht der Gesetzesentwurf neue Ausnahmen von den Sicherheitsvorgaben für das Auswärtige Amt (AA) und das Bundesministerium

der Verteidigung (BMVg) vor, die weit über die bestehenden Ausnahmen gemäß IT-SiG 2.0 hinausgehen. Sachgründe für diese geplante Erweiterung gibt es aus Sicht des BSI nicht. Die bestehenden Ausnahmen im BSIG für AA und BMVg sollten nicht erweitert werden, um einer Fragmentierung des Cybersicherheitsniveaus auf Bundesebene entgegenzuwirken.

⇨ *Empfehlung für einheitliche IT-Sicherheitsvorgaben für die gesamte Bundesverwaltung und Beibehaltung der bestehenden Ausnahmen für AA und BMVg:*

1. Die Begrifflichkeit "Einrichtungen der Bundesverwaltung" durch "*Einrichtungen des Bundes*" im gesamten Gesetz ersetzen.

2. Weitere Anpassungen:
   § 2 Abs. 1 BSIG-E um folgende Definition ergänzen:
   „9a. Einrichtungen des Bundes die Bundesbehörden, einschließlich derjenigen öffentlichen Stellen, die zur Erfüllung der öffentlichen Aufgaben dieser Behörden Informationstechnik betreiben."

   und es wird ergänzt:
   „Das Bundesamt kann für öffentliche Stellen, die nicht bereits Absatz 1 Nummer 9a unterfallen, im Benehmen mit der für diese Stelle zuständigen obersten Bundesbehörde feststellen, dass die Stelle eine Einrichtung des Bundes im Sinne dieses Gesetzes ist, wenn sich andernfalls Risiken für die Informationstechnik des Bundes ergeben."

   § 29 BSIG-E wird ersetzt mit:
   „(1) Für Einrichtungen des Bundes, die nicht von § 28 erfasst sind, gelten die Pflichten für besonders wichtige Einrichtungen dieses Teils entsprechend.

   (2) Die Ausnahmen nach § 7 Absätze 6 und 7 gelten für die Pflichten nach diesem Teil entsprechend."

   und in § 28 Abs. 1 BSIG-E wird Satz 2 gestrichen:
   „~~Davon ausgenommen sind Einrichtungen der Bundesverwaltung, sofern sie nicht gleichzeitig Betreiber kritischer Anlagen sind~~."

   und in § 28 Abs. 2 BSIG-E wird Satz 2 gestrichen:
   „~~Davon ausgenommen sind besonders wichtige Einrichtungen und Einrichtungen der Bundesverwaltung~~."

b) Klarstellung der Pflichten und Mittelallokation für Informationssicherheit

Damit Nachweispflichten für die Einrichtungsleitungen in der Bundesverwaltung nicht durch fehlende Bestimmung ins Leere laufen, ist eine rechtliche Erläuterung notwendig, was mit „Gewährleistung der Informationssicherheit" gemeint ist. Durch klare Vorgaben wird Rechtssicherheit geschaffen. Ergänzend dazu sollte festgehalten werden,

dass zur Gewährleistung der Informationssicherheit auch die Bereitstellung einer angemessenen Finanzierung zählt.

⇨ *Empfehlung zur Ergänzung § 43 Abs. 1 BSIG-E um nachfolgende Sätze 2 und 3:*

„Die Informationssicherheit wird grundsätzlich durch die Einhaltung der Risikomanagementpflichten nach § 30 gewährleistet. Zu den Voraussetzungen zur Gewährleistung der Informationssicherheit zählt der Einsatz angemessener finanzieller Mittel."

c) Möglichkeit zur flexiblen Anpassung der Sicherheitsvorgaben durch BSI

Damit das BSI die erforderlichen Sicherheitsvorgaben für die Bundesverwaltung an technologische Weiterentwicklungen zeitnah anpassen kann, sollte keine rechtliche Festlegung ausschließlich auf Mindestandards und IT-Grundschutz erfolgen. Vielmehr sollte das Gesetz technologieoffen ausgestaltet sein und stattdessen den Begriff der „Vorgaben" verwenden. Durch die unten vorgeschlagene Anpassung im Regierungsentwurf würde ein einheitlicher Schutzstandard für alle gesellschaftskritischen Tätigkeiten, unabhängig davon, ob Staat oder Wirtschaft, etabliert. Gleichzeitig bleibt es dem BSI möglich, verwaltungsintern weitere bedarfsgerechte Vorgaben zu machen, bspw. für die digitale Verarbeitung von Verschlusssachen in IT-Systemen.

⇨ *Empfehlung zur Anpassung des § 44 BSIG-E:*

Die bisherigen § 44 Absätze 1-3 werden mit einem neuen Absatz 1 ersetzt:

„(1) Soweit erforderlich legt das Bundesamt im Benehmen mit den Ressorts Vorgaben für die Sicherheit der Informationstechnik des Bundes zu den nach § 30 zu erfüllenden Anforderungen für die Einrichtungen des Bundes fest. Für die in § 2 Absatz 1 Nummer 18 genannten Gerichte und Verfassungsorgane haben die Vorschriften nach Satz 1 empfehlenden Charakter."

Absatz 4 wird zu Absatz 2;

Absatz 5 wird Absatz 3;

und § 44 Absatz 6 wird zu Absatz 4 und wie folgt gefasst:

„(4) Die oder der Bundesbeauftragte für Informationssicherheit kann im Benehmen mit den Ressorts festlegen, dass die Einrichtungen des Bundes verpflichtet sind, nach § 19 bereitgestellte IT-Sicherheitsprodukte beim Bundesamt abzurufen. Eigenbeschaffungen sind in diesem Fall nur zulässig, wenn das spezifische Anforderungsprofil den Einsatz abweichender Produkte erfordert. Dies gilt nicht für die in § 2 Nummer 21 genannten Gerichte und Verfassungsorgane."

7 Schwachstellenmanagement des BSI

Aus fachlicher Sicht des BSI sollten Sicherheitslücken grundsätzlich dem koordinierten Prozess zur Schließung zugeführt werden. Dies erfüllt das BSI bereits über seinen etablierten CVD-Prozess. Um die Unabhängigkeit des BSI bei dieser Aufgabe sicherzustellen und den Anreiz zur Meldung von Schwachstellen an das BSI zu erhöhen, sollte sichergestellt werden, dass das BSI bei der Meldung von Sicherheitslücken an Hersteller keinen Weisungen durch das BMI unterliegt. Aus fachlicher Sicht des BSI sollten hierfür nachfolgende Änderungen umgesetzt werden:

- ⇨ *Empfehlung zur Anpassung von § 5 BSIG-E:*

  An § 5 Abs. 1 BISG-E wird folgender Satz angefügt:
  „Das Bundesamt wirkt unverzüglich auf die Behebung von Schwachstellen hin."

  An § 5 Abs. 5 BSIG-E wird folgender Satz angefügt:
  „Weisungen an das Bundesamt, die eine Weitergabe von Informationen über Sicherheitslücken in Produkten an den Hersteller dieser Produkte untersagen, sind unzulässig."

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
20(4)523 D

Boehringer Ingelheim

Stellungnahme

Für die Anhörung des Deutschen Bundestages zum Entwurf der Bundesregierung eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (NIS2UmsuCG-E), BT-Drucksache 20/13184

Anhörung des Ausschusses für Inneres und Heimat des Deutschen Bundestages am 4. November 2024 um 11:00 Uhr

Sehr geehrte Damen und Herren Abgeordnete,

wir bedanken uns für die Einladung zu der oben genannten Anhörung im Rahmen des Gesetzgebungsverfahrens zur Umsetzung der europäischen NIS-2-Richtlinie durch die Bundesrepublik Deutschland.

Zu dem Gesetzentwurf der Bundesregierung nehmen wir wie folgt Stellung:

Als Hersteller von Arzneimitteln und Medizinprodukten und Unternehmen, die Forschungs- und Entwicklungstätigkeiten in Bezug auf Arzneimittel betreiben, fallen zumindest alle großen Pharmaunternehmen in Deutschland als „wichtige“ bzw. „besonders wichtige Einrichtungen“ in den Anwendungsbereich der NIS-2-Richtlinie beziehungsweise des geplanten deutschen Umsetzungsgesetzes.

Viele Unternehmen investieren bereits jetzt in erheblichem Umfang in Maßnahmen zur Gewährleistung eines hohen Cybersicherheitsniveaus, nicht zuletzt, um ihre Lieferketten stabil zu halten und um zu verhindern, dass wertvolles Know-how und Geschäftsgeheimnisse ins Ausland abfließen. Daher begrüßen wir die Absicht der Kommission, das Cybersicherheitsniveau in der Europäischen Union flächendeckend zu erhöhen und stärker zu harmonisieren, indem beispielsweise zu implementierende Risikomanagement-Maßnahmen verbindlich vorgeschrieben und gesetzlich konkretisiert werden.

Bevor wir uns zu einzelnen Bestimmungen äußern, möchten wir grundsätzlich dafür plädieren, bei der Umsetzung die Mindestanforderungen der NIS-2-Richtlinie nicht zu überschreiten. Hintergrund ist, dass europaweit bzw. global agierende Unternehmensgruppen oft mit einer einheitlichen, zentral gesteuerten IT-Landschaft arbeiten, in der Maßnahmen zum Risikomanagement, zur IT-Sicherheit sowie zu Meldeprozessen nicht länderbezogen, sondern in operativ sinnvoller Weise europaweit einheitlich implementiert sind. Ein solch zentraler Ansatz führt zur Erhöhung der IT-Sicherheit und ist gleichzeitig deutlich effizienter als eine dezentrale IT-Landschaft und -Organisation. Dieser Ansatz wird gefährdet, wenn Mitgliedstaaten über die NIS-2-Richtline hinausgehende Pflichten vorsehen. Daher plädieren wir dafür, komplexitätssteigernde überschießende Regelungen zu streichen und damit unnötige Bürokratie und

Aufwände auf Unternehmensseite zu vermeiden. Wir sind überzeugt, dass auf diesem Weg die Zielsetzungen der Gewährleistung eines hohen Cybersicherheitsniveaus in der EU und der Förderung der Attraktivität des Wirtschaftsstandorts Deutschland am effizientesten erreicht werden können.

Im Einzelnen möchten wir für eine Anpassung oder Streichung folgender Regelungen des vorliegenden Entwurfs plädieren:

1. **Sonderregelungen für Betreiber kritischer Anlagen – nicht erforderlich**

   Die Sonderregelungen für Betreiber kritischer Anlagen sind systemfremd, signifikant komplexitätssteigernd und im Ergebnis nicht erforderlich. Wir regen daher an, die entsprechenden Regelungen aus dem NIS2UmsuCG-E zu streichen.

   Mit dem NIS2UmsCG-E wird ein Systemwechsel gegenüber der Regulierung kritischer Infrastrukturen nach dem bestehenden BSIG vollzogen: Bezugspunkt sind nicht mehr (kritische) Infrastrukturen und deren Schutz, sondern Unternehmen/Institutionen und deren Dienste. Die Übernahme und Integration der bisherigen Kategorie der (Betreiber von) kritischen Infrastrukturen (bzw. jetzt "kritischen Anlagen") in das neue einrichtungsbezogene System des BSIG-E führt zu einem systematischen Bruch, der zu Interpretationsschwierigkeiten in vielerlei Hinsicht führt, z. B. in Bezug auf die Frage, ob die verschärften Anforderungen für Betreiber kritischer Anlagen für die gesamte Einrichtung oder nur für den Betrieb der kritischen Anlage Geltung beanspruchen.

   Darüber hinaus erhöht die unionsrechtlich nicht geforderte Kategorie der Betreiber kritischer Anlagen die Komplexität für Unternehmen in Bezug auf die Anwendbarkeitsprüfung und Umsetzung der Anforderungen erheblich. So wird eine belastbare Anwendbarkeitsprüfung unter dem derzeit geplanten BSIG-E erst dann möglich sein, wenn auch die finale Fassung der Verordnung nach § 56 Abs. 4 BSIG-E feststeht.

   Und auch danach erfordert das geplante Festhalten an sektorspezifischen Schwellenwerten über ein unternehmensseitiges Monitoring der allgemeinen Schwellenwerte der KMU-Empfehlung hinaus auch ein permanentes Monitoring von Versorgungskennzahlen. Im Falle einer Überschreitung der definierten Versorgungskennzahlen soll dann, den Vorgaben nach § 31 Abs. 1 BSIG-E entsprechend, ad hoc ein verschärfter Verhältnismäßigkeitsmaßstab für die zu implementierenden Risikomanagementmaßnahmen gelten. Dieses "Alles-oder-Nichts"-Prinzip, das im pharmazeutischen Bereich im Fall einer zusätzlich produzierten Packung Arzneimittel zu einem verschärften Risikomanagementmaßstab führen kann, ist aus Verhältnismäßigkeitsgesichtspunkten und Praktikabilitätserwägungen nicht zielführend.

   Darüber hinaus ist die Sonderregelung des § 31 Abs. 1 BSIG-E nicht erforderlich, da eine erhöhte gesellschaftliche oder wirtschaftliche Bedeutung einer bestimmten Dienstleistung bereits im Zuge der allgemeinen für besonders wichtige und wichtige Einrichtungen geltenden Risikomanagementanforderungen zu berücksichtigen ist und bereits auf Grundlage des § 30 Abs. 1 BSIG-E zu einer Anhebung des geforderten Schutzniveaus führt.

Die vorstehenden Ausführungen gelten entsprechend für die Verpflichtung zum Einsatz von Angriffserkennungssystemen in § 31 Abs. 2 BSIG-E. Soweit von dieser Regelung besonders wichtige oder wichtige Einrichtungen betroffen sind, die in den Anwendungsbereich der Durchführungsverordnung (EU) 2024/2690 fallen (wie zum Beispiel Anbieter von Cloud Computing-Diensten), begegnet die Vorschrift zudem unionsrechtlichen Bedenken: Sie widerspricht der in Erwägungsgrund 84 der NIS-2-Richtlinie verankerten unionsrechtlichen Intention eines hohen Maßes an Harmonisierung in den erfassten digitalen Sektoren, da sich die Anforderungen aus § 31 Abs. 2 BSIG-E i.V.m. § 2 Nr. 41 BSIG-E nicht mit den in Nummer 3.2.1 des Anhangs der vorstehend genannten Durchführungsverordnung konkretisierten Anforderungen an Überwachung und Protokollierung decken.

Ebenfalls nicht erforderlich, jedoch ein signifikantes Maß an Bürokratie generierend, ist die in § 39 BSIG-E verankerte periodische Nachweispflicht für Betreiber kritischer Anlagen. Wir halten insofern die gegenüber besonders wichtigen Einrichtungen bestehenden Aufsichtsbefugnisse des BSI, die eine anlasslose Anordnung der Durchführung von Audits, Prüfungen oder Zertifizierungen von unabhängigen Stellen (siehe § 61 Abs. 1 BSIG-E) oder der Vorlage von Nachweisen über die Einhaltung der Risikomanagementpflichten (siehe § 61 Abs. 3 BSIG-E) erlauben, für ausreichend.

Sofern weiterhin an den Sonderregelungen für Betreiber kritischer Anlagen festgehalten werden sollte, sollte in § 56 Abs. 4 BSIG-E jedenfalls eine Anhörungspflicht aufgenommen werden, um sicherzustellen, dass die relevanten Interessengruppen Stellung nehmen können, bevor in der entsprechenden Verordnung die als kritisch anzusehenden Dienstleistungen und deren als bedeutend anzusehende Versorgungsgrade definiert werden. Eine derartige Bestimmung, die die *„Anhörung von Vertretern der Wissenschaft, der betroffenen Betreiber und der betroffenen Wirtschaftsverbände“* vorsieht, ist de lege lata auch in § 10 Abs. 1 BSIG enthalten.

2. Nationale Spezifizierungen von Risikomanagementmaßnahmen sollten sich auf internationale Standards und Normen beziehen

Die in § 30 Abs. 5 BSIG geregelte Verordnungsermächtigung des Bundesministeriums des Inneren und Heimat ("BMI") sollte auf eine Präzisierung der nach § 30 Abs. 1 und 2 BSIG geforderten Risikomanagementmaßnahmen beschränkt und um ein Anhörungserfordernis sowie um die Pflicht des BMI, sich bei der Ausarbeitung der Verordnung so weit wie möglich an europäischen und internationalen Normen sowie einschlägigen technischen Spezifikationen zu orientieren, ergänzt werden.

§ 30 Abs. 5 BSIG-E erlaubt es dem BMI – jenseits abschließender unionsrechtlicher Durchführungsrechtsakte der Europäischen Kommission nach Art. 21 Abs. 5 der NIS-2-Richtlinie – eine Präzisierung und Erweiterung der von § 30 Abs. 2 BSIG-E geforderten Risikomanagementmaßnahmen vorzunehmen.

Wir plädieren im Sinne einer möglichst umfassenden unionsweiten Harmonisierung der Cybersicherheitsvorgaben dafür, die Verordnungsermächtigung auf die Befugnis zur Präzisierung der

Vorgaben des § 30 Abs. 2 BSIG zu beschränken und keine Erweiterung der Managementmaßnahmen auf dem Verordnungsweg zu eröffnen.

Jedenfalls sollte das BMI in § 30 Abs. 5 BSIG-E verpflichtet werden, sich bei der Ausarbeitung der Verordnung so weit wie möglich an europäischen und internationalen Normen sowie einschlägigen technischen Spezifikationen zu orientieren. Die Europäische Kommission unterliegt im Rahmen ihrer delegierten Rechtsetzung ebenfalls einer entsprechenden Vorgabe (siehe Art. 21 Abs. 5 UAbs. 3 NIS-2-Richtlinie).

Zudem sollte die Verordnungsermächtigung des § 30 Abs. 5 BSIG-E um eine Anhörungspflicht ergänzt werden. Wir halten auch hier die Beteiligung von Vertretern der Wissenschaft, der betroffenen Betreiber und der betroffenen Wirtschaftsverbände für angezeigt, um eine praxistaugliche und an der Unternehmensrealität orientierte Spezifizierung der Risikomanagementmaßnahmen zu gewährleisten.

3. Governance- und Schulungspflichten durch Geschäftsleitungen in § 38 BSIG-E sollten nachgeschärft werden

§ 38 BSIG-E ist in der gegenwärtigen Entwurfsfassung missverständlich und sollte wie in der NIS-2-Richtlinie gefasst werden, um die bestehenden Rechtsunsicherheiten zu beseitigen.

Dem Wortlaut von § 38 Abs. 1 BSIG-E zufolge sind "*Geschäftsleitungen besonders wichtiger Einrichtungen und wichtiger Einrichtungen […] verpflichtet, die von diesen Einrichtungen […] zu ergreifenden Risikomanagementmaßnahmen umzusetzen und ihre Umsetzung zu überwachen*". Wir halten diese Formulierung in zweierlei Hinsicht für missverständlich.

Zum einen suggeriert der Wortlaut "*umzusetzen*", dass eine Umsetzung der Maßnahmen durch die Leitungsebene selbst erfolgen müsse. Abweichend hiervon wird in der Gesetzesbegründung ausgeführt, dass Geschäftsleitungen die konkret zu greifenden Maßnahmen "*als für geeignet zu billigen*" haben und auch dann letztverantwortlich für die Geeignetheit und Umsetzung erforderlicher Maßnahmen bleiben, wenn Hilfspersonen eingeschaltet, also zum Beispiel Aufgaben an einen Informationssicherheitsbeauftragten delegiert werden. Da eine Umsetzung durch die Leitungsebene in persona nicht der Intention des § 38 Abs. 1 BSIG-E entsprechen kann, regen wir an, die Formulierung "*umzusetzen*" mit der Formulierung "*als für geeignet zu billigen*" oder – entsprechend der Formulierung in Artikel 20 Abs. 1 NIS-2-Richtlinie – mit dem Wortlaut "*zu billigen*" zu ersetzen.

Zum anderen führt die Verwendung des Begriffs "*Geschäftsleitungen*" in § 38 BSIG-E in Verbindung mit der Legaldefinition des Begriffs der "*Geschäftsleitung*" in § 2 Nr. 13 BSIG-E zu vermeidbaren Unschärfen der Vorgaben in § 38 BSIG-E. Vor dem Hintergrund, dass § 2 Nr. 13 BSIG-E den Begriff der Geschäftsleitung als "*eine natürliche Person, die nach Gesetz, Satzung oder Gesellschaftsvertrag zur Führung der Geschäfte und zur Vertretung einer besonders wichtigen Einrichtung oder wichtigen Einrichtung berufen ist,*" definiert und § 38 BSIG-E stets auf den Plural "*Geschäftsleitungen*" rekurriert, scheint § 38 BSIG-E dem Wortlaut zufolge stets alle Mitglieder der Leitungsebene zu adressieren und allen Mitgliedern die entsprechenden Überwachungs- und

Schulungspflichten sowie die mit der Überwachungspflicht korrelierende Binnenhaftung nach § 38 Abs. 2 BSIG-E aufzuerlegen.

Da dies im Widerspruch zu gesellschaftsrechtlichen Vorgaben und der gelebten Leitungspraxis steht, sollte insofern klargestellt werden, dass § 38 BSIG-E einer geschäftsleitungsinternen Allokation der Zuständigkeit für das Thema Cybersicherheit im Rahmen einer Ressortaufteilung nicht entgegensteht und in einem solchen Fall ausschließlich der mit dieser Aufgabe betraute Geschäftsführer der jeweiligen besonders wichtigen oder wichtigen Einrichtung den Überwachungs- und Schulungspflichten des § 38 Abs. 1 und 3 BSIG-E sowie der Binnenhaftung nach § 38 Abs. 2 BSIG-E unterliegt.

Wir regen insofern an, anstelle des Plurals "*Geschäftsleitungen*" in § 38 BSIG-E den Singular "*Geschäftsleitung*" zu verwenden und die Legaldefinition in § 2 Nr. 13 BSIG-E wie folgt anzupassen:

> *„Geschäftsleitung“ eine natürliche Person **oder mehrere natürliche Personen**, die nach Gesetz, Satzung oder Gesellschaftsvertrag zur Führung der Geschäfte und zur Vertretung einer besonders wichtigen Einrichtung oder wichtigen Einrichtung berufen ist **oder sind**;*

Adressat der Verpflichtungen aus § 38 BSIG-E wäre damit das Organ der Geschäftsleitung als solches und nicht die einzelnen Personen dieses Organs. Einer Zuständigkeitsallokation innerhalb der Geschäftsleitung stünde die Regelung in der Folge nicht mehr entgegen.

4. Verweis auf § 30 Abs. 2 Satz 3 OWiG im Falle der Verletzung der Nachweispflicht nach § 39 Abs. 1 Satz 1 BSIG-E unverhältnismäßig

In den Bußgeldregelungen wird in § 65 Abs. 5 Satz 2 BSIG-E für bestimmte Verstöße gegen die Vorschriften des BSIG-E auf die Regelung des § 30 Abs. 2 Satz 3 OWiG verwiesen. Diesen Verweis, der zu einer Verzehnfachung des jeweils angedrohten Höchstmaßes des Bußgeldes führt, halten wir für Verstöße gegen die in § 39 Abs. 1 Satz 1 BSIG geregelte Nachweispflicht für nicht verhältnismäßig.

Wir regen daher an, den Verweis auf Satz 1 Nr. 3 in § 65 Abs. 5 Satz 2 BSIG-E zu streichen.

5. Dokumentationserfordernis in § 30 Abs. 1 Satz 3 BSIG-E sollte gestrichen werden

Die in § 30 Abs. 1 Satz 3 BSIG-E geregelte Verpflichtung, die Einhaltung der Verpflichtung nach § 30 Abs. 1 Satz 1 BSIG-E zu dokumentieren, sollte gestrichen werden.

Die Dokumentationspflicht in § 30 Abs. 1 Satz 3 BSIG-E ist in ihrem Umfang zu unbestimmt und schafft unnötige Bürokratie. Sie ist darüber hinaus nicht erforderlich, da besonders wichtige Einrichtungen gemäß § 61 Abs. 3 BSIG-E auch ohne eine solche Dokumentationspflicht verpflichtet sind, auf Anforderung des Bundesamts für Sicherheit in der Informationstechnik einen Nachweis über die Erfüllung der geforderten Risikomanagementmaßnahmen zu erbringen.

6. Öffentlichkeitsbeteiligung auch hinsichtlich der Verordnungsermächtigungen in § 56 Abs. 3 und 5 BSIG-E

Analog zu unseren Forderungen zu den Verordnungsermächtigungen in § 30 Abs. 5 BSIG-E und § 56 Abs. 4 BSIG-E regen wir auch bezüglich der Ermächtigungsgrundlagen in § 56 Abs. 3 und 5 BSIG-E an, eine Verpflichtung zur Anhörung von Vertretern der Wissenschaft, der betroffenen Betreiber und der betroffenen Wirtschaftsverbände aufzunehmen.

Eine Beteiligung dieser Kreise ist aus unserer Sicht auch in diesen Bereichen unerlässlich, um wissenschaftliche Expertise und Praxiserfahrungen in dem erforderlichen Umfang in die Ausarbeitung der entsprechenden Verordnungen einfließen zu lassen und eine praxistaugliche und gleichzeitig ein hohes Schutzniveau gewährleistende Ausgestaltung der entsprechenden Vorgaben sicherzustellen.

7. Konkretisierung der Regelungen zur Berechnung der relevanten Einrichtungskennzahlen

In der Regelung zur Berechnung der relevanten Einrichtungskennzahlen (§ 28 Abs. 3 BSIG-E) sollte klargestellt werden, ob die geschäftstätigkeitsbezogene Betrachtung, wie sie in § 28 Abs. 3 Satz 1 Nr. 1 BSIG-E vorgeschrieben wird, auch für die Zurechnung von Kennzahlen verbundener Unternehmen und Partnerunternehmen gilt.

§ 28 Abs. 3 Satz 1 Nr. 1 BSIG-E schreibt vor, dass "*bei der Bestimmung von Mitarbeiteranzahl, Jahresumsatz und Jahresbilanzsumme […] auf die der Einrichtungsart zuzuordnende Geschäftstätigkeit abzustellen*" ist.

In der Gesetzesbegründung wird hierzu ausgeführt, dass "*bei der Bestimmung der maßgeblichen Mitarbeiterzahlen und des Umsatzes […] nur diejenigen Teile der Einrichtung einzubeziehen [sind], die tatsächlich im Bereich der in den Anlagen 1 und 2 genannten Definitionen der Einrichtungskategorien tätig sind [und dass] Querschnittsaufgaben wie beispielsweise Personal, Buchhaltung etc. […] hierbei anteilig zu berücksichtigen [sind].*" Hierdurch soll "*sichergestellt [werden], dass Einrichtungen, die insgesamt die Größenschwelle für Mitarbeiteranzahl, Jahresumsatz oder Jahresbilanzsumme überschreiten, deren hauptsächliche Geschäftstätigkeit jedoch nicht einer Einrichtungskategorie gemäß Anlage 1 oder 2 dieses Gesetzes zuzuordnen ist, nicht in unverhältnismäßiger Weise erfasst werden*".

Angesichts der auf einzelne juristische Personen bezogenen Legaldefinition von Einrichtungen in § 28 Abs. 1 Nr. 4 und Abs. 2 Nr. 3 BSIG-E verstehen wir die Regelung in § 28 Abs. 3 Satz 1 Nr. 1 BSIG dahingehend, dass diese für die isolierte Betrachtung einer juristischen Person gelten soll.

Offen bleibt indes, ob die auf die erfasste Geschäftstätigkeit beschränkte Betrachtung auch für die unter § 28 Abs. 3 Satz 1 Nr. 2 BSIG-E i.V.m. der KMU-Empfehlung vorzunehmende Zurechnung von Mitarbeiteranzahl, Jahresumsatz und Jahresbilanzsumme gelten soll. Hierfür spricht, dass sich die vorstehend zitierte Argumentation aus der Gesetzesbegründung auch auf die Zurechnung von Daten verbundener Unternehmen übertragen lässt.

Die insofern bestehende Regelungslücke, die die aufgrund der Verweisungssystematik der Anhänge 1 und 2 ohnehin bestehenden Rechtsunsicherheiten im Rahmen der Anwendbarkeitsprüfung erheblich verstärkt, sollte durch eine Klarstellung geschlossen werden.

***

Stellungnahme von Dr. Sven Herpig, Lead Cybersecurity Policy and Resilience bei interface (ehemals: Stiftung Neue Verantwortung), für die öffentliche Anhörung des Ausschusses für Inneres und Heimat des Deutschen Bundestags am 4. November 2024 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 20/13184)

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
20(4)523 E

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

Inhaltsverzeichnis

1. Vorbemerkungen

Beim NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS-2UmsuCG) handelt es sich um die nationale Transposition der zweiten EU-Richtlinie über die Sicherheit von Netzen und Informationssystemen (NIS-2-Richtlinie). Das NIS-2UmsuCG 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. Hinzu kommt, dass es sich bei diesem Gesetzesvorhaben um vermutlich eine der letzten Möglichkeiten der Bundesregierung handelt, legislative Vorhaben, die sich aus dem Koalitionsvertrag ergeben, umzusetzen – sofern sie sich mit dem Regelungsbereich der NIS-2-Richtlinie decken. Zusammenfassend handelt es sich bei diesem Gesetzgebungsvorhaben somit um einen komplexen Prozess, was sich unter anderem in einer kompletten Neufassung des Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (zukünftig "Gesetz über das Bundesamt für Sicherheit in der Informationstechnik und über die Sicherheit in der Informationstechnik von Einrichtungen", BSIG) widerspiegelt.

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, mehr IT-Sicherheit herzustellen. 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, was 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-2UmsuCG ist nicht das Ende eines umfassenden Vorhabens für mehr 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 (NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz)" vom 02.10.2024 (Drucksache 20/13184) angeregt. Die Empfehlungen erfolgen aus inhaltlicher, nicht aus rechtlicher Betrachtung. Es wird vorgeschlagen, die vom Bundesministerium des Innern und für Heimat im bisherigen und zukünftigen Gesetzgebungsprozess als Argument gegen Änderungsvorschläge Dritter geäußerten verfassungsrechtlichen Bedenken[2] unabhängig prüfen zu lassen. Hintergrund ist, dass die Exekutive in der Vergangenheit bei Sicherheitsgesetzen verfassungsrechtliche Grenzen überschritten hat, weshalb ihre Beurteilungen zumindest überprüft werden sollten.[3]

[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)
[2] Bundesregierung (2024): Stellungnahme der Bundesregierung zur Stellungnahme des Nationalen Normenkontrollrates
[3] Siehe zum Beispiel Anke Domscheit-Berg (2021): Bundesregierung will Überwachungsgesetze nicht überprüfen oder Constanze Kurz (2024): BKA-Gesetz erneut in Teilen verfassungswidrig

2.1. IT-Sicherheitsregulierung für Bund und Länder

Nachdem es bisher verpasst wurde eine Cybersicherheitsarchitektur[4] 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.

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

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

2.2. Staatlicher Umgang mit Schwachstellen

Im Koalitionsvertrag heißt es: “Wir führen[...] ein wirksames Schwachstellenmanagement, mit dem Ziel, Sicherheitslücken zu schließen, [...] ein”. Der Sachverständige hat hierzu einen Vorschlag vorgelegt[5] und in einer

[4] interface (2024): Cybersicherheitsarchitektur
[5] Sven Herpig (2018): Schwachstellen-Management für mehr Sicherheit und Sven Herpig (im Erscheinen): Vulnerability Disclosure: Guiding Governments from Norm to Action

Sachverständigenstellungnahme[6] 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.

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 Satz 4 BSIG-E.

2.3. Detailänderungen

§ 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 der Landesverwaltungen Unternehmen, Verbraucher:innen und anderen nicht auf Grundlage 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.[7]

[6] 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".
[7] 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".

§ 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 Mehraufwand ohne erkennbaren Mehrwert für die IT-Sicherheit geschaffen.

§ 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.

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.

§ 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.

§ 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, da wo möglich 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.

§ 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: 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.

§ 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.

§ 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 für Sicherheitsforscher:innen abgebaut werden, Schwachstellen an das Bundesamt zu melden.

§ 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.

§ 6 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.

§ 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.

§ 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.

§ 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 deren Funktion hierdurch nicht unverhältlnismäßig beeinträchtigt wird, […]”

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.

§ 16 BSIG-E

Wortlaut: Ergänzung

Empfehlung: "(5) Nach Absatz 1 angeordnete Maßnahmen müssen protokolliert und zur Information von Abgeordneten in der Geheimschutzstelle des Bundestags einsehbar sein."

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

§ 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.

§ 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 des Innern und für Heimat 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.

§ 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 Satz 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 des Innern und für Heimat 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 Satz 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, das Bundeskanzleramt erlassen im Einvernehmen mit dem Bundesministerium des Innern und für Heimat 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.

§ 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 können soll.

§ 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.

§ 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.

§ 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 erbringen sollen müssen.

§ 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. Sollte es sich hierbei um das Bundesamt handeln, siehe auch Empfehlung zu § 1 Satz 3 BSIG-E. Wichtig ist hierbei sicherzustellen, dass es eine fachliche Unabhängigkeit des:der Koordinators:in für Informationssicherheit von der:vom Beauftragten der Bundesregierung für Informationstechnik gibt.

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. Vorschläge zur Rolle des:der Koordinators:infür Informationssicherheit finden sich in der Stellungnahme des Sachverständigen.[8]

§ 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.

§ 56 Absatz 4 BSIG-E

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

Empfehlung: "Das Bundesministerium des Innern, und für Bau und Heimat 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.

[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".

3. Schlussbemerkungen

Der Sachverständige weist auf folgende Stellungnahmen der nicht in der Anhörung vertretenen Organisationen mit einschlägiger Expertise hin:

- Arbeitsgruppe Kritische Infrastrukturen (AG KRITIS): Stellungnahme zum Regierungsentwurf des NIS2UmsuCG vom 02.10.2024
- Gesellschaft für Datenschutz und Datensicherheit e.V. (GDD): Stellungnahme der GDD e.V. zum Entwurf der Bundesregierung für ein Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (NIS-2-Umsetzungsund Cybersicherheitsstärkungsgesetz) - BT-Drs. 20/13184

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.

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.

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
20(4)523 G

Universität Bremen

IGMR
Institut für Informations-, Gesundheits- und Medizinrecht

Universität Bremen | Postfach 33 04 40, 28334 Bremen
IGMR | **FB06**

Deutscher Bundestag
Ausschuss für Inneres und Heimat
- Sekretariat -
Platz der Republik 1
11011 Berlin

Fachbereich 06
Rechtswissenschaft

Prof. Dr. jur. Dennis-Kenji Kipker

Universitätsallee GW 1
28359 Bremen

Tel. 0421 5905 5465
Fax 0421 218 66052
kipker@uni-bremen.de

www.igmr.uni-bremen.de
igmr@uni-bremen.de

Bremen 31. Oktober 2024

Schriftliche Stellungnahme

zum

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

(BT-Drucksache 20/13184)

Zusammenfassung und Vorbemerkung:

Gemessen an der Tatsache, dass die Umsetzung von NIS2 in Deutschland schon seit mittlerweile fast zwei Jahren möglich ist und angegangen wird, enthält der vorgelegte Entwurf leider noch zu viele Schwächen und Unklarheiten, teilweise auch Maßgaben, die der Erhöhung des allgemeinen Cybersicherheitsniveaus nicht förderlich sind. Zu vermissen ist ebenfalls eine Vereinheitlichung der Systematik des nationalen Cybersicherheitsrechts, die zwischen bereichsspezifischen und allgemeinen Vorgaben und der Cybersicherheit in Bund und Ländern unterscheidet – denn letztlich verlangt NIS-2 nichts anderes, als dass selbst in einem föderalen Deutschland einheitliche Cybersicherheitsstandards definiert werden. Aufgrund der nach wie vor bestehenden Zersplitterung von Vorgaben verteilt auf unterschiedliche regulatorische Ebenen mit unterschiedlicher Verbindlichkeit sind wir weit von einer einheitlichen Umsetzung entfernt. Hier hätten die letzten Jahre eigentlich gezielt genutzt werden müssen und können, um eine stärkere politische Abstimmung zwischen Bund und Ländern zu erreichen. Auch werden verschiedene Punkte, die beispielsweise schon im Jahr 2023 bei Sitzungen der AG BSI adressiert wurden, nicht aufgegriffen. Damit hat man es mit dem vorgelegten Gesetzentwurf bislang leider versäumt, NIS-2 nicht nur zur Umsetzung eines europäischen Minimalstandards zu nutzen, sondern das nationale Cybersicherheitsrecht auf eine grundlegend solide Basis zu stellen, die Rechtsunsicherheit ausräumt und eine nachhaltige Entwicklung für die gesteigerte Bedrohungslage der kommenden Jahre schafft.

Hauptkritikpunkte betreffen dabei die nach wie vor im nationalen Verwaltungsgefüge unklare Rolle des BSI, die nicht angetastet wurde, obwohl das BSI nicht nur in seiner Rolle als Zentralstelle für Cybersicherheit einen massiven weiteren Ausbau erfahren soll, sondern mit NIS-2 auch

zahlreiche weitere Befugnisse erhalten wird. Jenseits von NIS-2 positioniert sich das BSI außerdem bereits jetzt für die nationale Umsetzung des europäischen Cyber Resilience Act (CRA), womit weitere ganz erhebliche Befugnisse einhergehen, die deutlich für eine größere Unabhängigkeit des BSI sprechen. Bereits mehrfach kritisierte begriffliche Schwächen, die sich bereits im geltenden Recht wiederfinden, werden nicht ausgeräumt – dies ist für den richtigen und rechtssicheren Umgang mit den Vorschriften durch die Betroffenen jedoch essenziell. Ganz zentral ist überdies die gesetzlich angeordnete Umsetzung von IT-Sicherheitsmaßnahmen nach NIS-2 in § 30 BSIG-E. Hier wird nahezu 1:1 auf den NIS-2-Maßnahmenkatalog verwiesen, was bei betroffenen Einrichtungen jedoch zu Unsicherheit darüber führt, welche Maßnahmen im Einzelnen zu realisieren sind und ob diese überhaupt in den konkreten betrieblichen Anwendungskontext passen. Zugegebenermaßen lässt hier bereits das europäische Recht mit einer willkürlich erscheinenden Aufzählung von Maßnahmen zur Cybersicherheit zu wünschen übrig, die nicht weiter konkretisiert werden, aber dennoch unmittelbare Pflicht sind. Im Ergebnis gerät dadurch jedoch zunehmend außer Fokus, dass Cybersicherheit eine Managementaufgabe ist, die sich an eine individuelle Risikobewertung anschließt, und deshalb zunächst nichts mit einzelnen Produkten und Insellösungen zur Cybersicherheit zu tun hat. Dasselbe gilt für die pauschale Anordnung zur Verwendung von Systemen zur Angriffserkennung. Diese Unsicherheit für betroffene Einrichtungen zieht sich bedauerlicherweise durch den gesamten Gesetzentwurf, so mit Blick auf die Anforderungen an Dokumentation und Nachweise, die Geschäftsleiterverantwortlichkeit sowie die Schaffung von betrieblicher Awareness und auch die Meldepflichten. Für letztere wird zum Beispiel auf „immaterielle Schäden“ verwiesen, ohne dass deutlich hervorgeht, was davon inhaltlich

umfasst sein soll und wie diese im Zweifelsfall von datenschutzrechtlichen Meldungen abzugrenzen sein sollen. Über den Bereich betroffener Privatunternehmen hinausgehend finden sich überdies auch im öffentlichen Teil des Gesetzesvorschlags weitere und auch systematische Schwächen, die an die Definition von Einrichtungen der Bundesverwaltung und an die künftige Rolle des CISO Bund anknüpfen.

Im Hinblick auf den Datenschutz enthält der Entwurf außerdem weitere erhebliche nennenswerte Schwächen, die teils sogar unionsrechtswidrig sein dürften, so zum Beispiel die Anforderung, nur „offensichtliche Datenschutzverletzungen“ infolge eines Cybersicherheitsvorfalls an die Datenschutzaufsicht zu melden und wie die Befugnisse von BSI und BfDI auch künftig klar voneinander abzugrenzen sein sollen.

Im Hinblick auf das bisherige Verfahren und die Beteiligung relevanter Akteure ist überdies zu kritisieren, dass die BfDI bislang nicht ausreichend einbezogen wurde, obwohl im Gesetzentwurf wie dargestellt massive Befugniserweiterungen des BSI zur (personenbezogenen) Datenverarbeitung im Raum stehen und deshalb auch datenschutzrechtliche Regelungen in erheblichem Maße tangiert sind. § 69a Abs. 3 GOBT sieht ein ausdrückliches und frühzeitiges Beteiligungsrecht der BfDI vor, das bei der nationalen Umsetzung von NIS2 bislang leider nicht ausgeübt wurde.

Zu den Vorschriften im Einzelnen:

- **§ 1 BSIG-E (Bundesamt für Sicherheit in der Informationstechnik):**

  § 1 BSIG bestimmt in der geltenden Fassung wie auch im Entwurf, dass das BSI eine Bundesoberbehörde im Geschäftsbereich des Bundesinnenministeriums und zentrale Stelle für Informationssicherheit auf nationaler Ebene ist. In dieser Funktion führt es seine Aufgaben gegenüber den Bundesministerien auf der Grundlage von wissenschaftlich-technischen Erkenntnissen durch. Nach wie vor ist bei dieser gewählten Formulierung unklar, weshalb sie trotz bereits seit mehreren Jahren geäußerter Kritik keine Anpassung erfährt. Dies betrifft einerseits die Rolle des BSI und dessen Forderung nach institutioneller Unabhängigkeit, zu deren Zwecken unter anderem auch die „AG BSI“ eingerichtet wurde. Dabei ist es zwingend notwendig, dass im Zuge der stetig und in den vergangenen Jahren massiv erweiterten behördlichen Befugnisse eine zeitnahe Lösung gefunden wird. Der Verfasser dieser Stellungnahme hat entsprechende Vorschläge nicht nur in einer Sitzung der AG BSI am 8. September 2023 persönlich zur Diskussion gestellt, sondern in Ko-Autorenschaft auch einen entsprechenden Fachbeitrag publiziert, der konkrete rechtliche Möglichkeiten zur Unabhängigstellung des BSI in gradueller Abstufung aufzeigt (Kipker/Mayr, Zur Unabhängigkeit des BSI: Die juristische Analyse einer politischen Debatte, DuD 2023, 790-795, online abrufbar unter: https://link.springer.com/article/10.1007/s11623-023-1864-z). Andererseits lässt sich mittels sachlicher Argumentation nicht recht-

fertigen, weshalb das BSI ausschließlich „gegenüber den Bundesministerien“ seine Aufgaben auf der „Grundlage wissenschaftlich-technischer Erkenntnisse“ durchführt. Das BSI ist eine Fachbehörde und hat deshalb seine Aufgaben gegenüber allen betroffenen Einrichtungen nach diesem Maßstab auszuführen – zumal aus dem Wortlaut der Vorschrift nicht hervorgeht, was die alternativen Handlungsmaßstäbe des BSI gegenüber den anderen auch durch das Gesetz betroffenen Einrichtungen wären. Im Ergebnis geht es somit darum, Komplexitäten in der Aufgabenwahrnehmung zu reduzieren, zentrale und verlässliche Entscheidungswege zu etablieren und Verfahren nationaler Informationssicherheit effizienzsteigernd orientiert am größtmöglichen Nutzen für die Informationssicherheit auszugestalten.

- **§ 2 Nr. 10 BSIG-E (Begriffsbestimmungen, hier: „erhebliche Cyberbedrohung“):**

  Für die Definition der „einfachen“ Cyberbedrohung wird zur Konkretisierung zur Förderung eines einheitlichen begrifflichen Verständnisses richtigerweise auf Art. 2 Nr. 8 der Verordnung (EU) 2019/881 (Cybersecurity Act) verwiesen. Danach bezeichnet eine Cyberbedrohung einen möglichen Umstand, ein mögliches Ereignis oder eine mögliche Handlung, der/das/die Netz- und Informationssysteme, die Nutzer dieser Systeme und andere Personen schädigen, stören oder anderweitig beeinträchtigen könnte. Eine „erhebliche Cyberbedrohung“ soll demgegenüber eine Cyberbedrohung sein, die das Potenzial besitzt, die informationstechni-

schen Systeme, Komponenten und Prozesse aufgrund der besonderen technischen Merkmale der Cyberbedrohung erheblich zu beeinträchtigen. Eine solche erhebliche Beeinträchtigung liegt laut Entwurf dann vor, wenn sie erheblichen materiellen oder immateriellen Schaden verursachen kann. Diese verwendete Formulierung ist aus zweierlei Gründen zu unbestimmt und sollte deshalb konkretisiert werden: So geht nicht deutlich aus der Vorschrift hervor, wie die „Erheblichkeit" vom „Regelfall" anzugrenzen ist und welche Ressourcen für diesen Fall zur Bewältigung der Cyberbedrohung herangezogen werden sollen. Überdies ist rechtlich unbestimmt, was mit einem „immateriellen Schaden" gemeint sein soll und wie sich dieser bemerkbar macht bzw. auch von einem Datenschutzvorfall infolge einer realisierten Cyberbedrohung abzugrenzen ist. Dadurch entsteht das Risiko missverstandener oder zu weit ausgelegter Meldemaßnahmen von Unternehmen als unmittelbare Folge einer Rechtsunsicherheit. Dies führt zu ersparenswerten Mehraufwänden sowohl auf der Seite der durch NIS2UmsuCG betroffenen wie auch der beteiligten Behörden.

- **§ 2 Nr. 11 BSIG-E (Begriffsbestimmungen, hier: „erheblicher Sicherheitsvorfall"):**

  Die für die vorgenannten Definition „erhebliche Cyberbedrohung" genannten rechtlichen Probleme setzen sich bei der Definition des „erheblichen Sicherheitsvorfalls" fort, denn insbesondere in der zweiten Variante lit. b) liegt ein solcher Vorfall dann vor, wenn er andere natürliche oder juristische Personen durch erhebliche

materielle oder immaterielle Schäden beeinträchtigt hat oder beeinträchtigen kann. So ist auch hier unklar, was mit „erheblichen“ Schäden sowie mit „immateriellen“ Schäden im Kontext des IT-Sicherheitsrechts gemeint sein soll. In der Praxis dürfte überdies generell die „erhebliche Cyberbedrohung“ vom „erheblichen Sicherheitsvorfall“ nur schwer begrifflich abgrenzbar sein, soweit sich die Beeinträchtigung bzw. Betriebsstörung noch nicht realisiert hat. Unabhängig von einer konkretisierenden Rechtsverordnung sollten hier weitere Bemessungskriterien ausgeführt werden.

- **§ 2 Nr. 12 BSIG-E (Begriffsbestimmungen, hier: „Forschungseinrichtung“):**

  Laut Definition ist eine Forschungseinrichtung eine Einrichtung, deren primäres Ziel es ist, angewandte Forschung oder experimentelle Entwicklung im Hinblick auf die Nutzung der Ergebnisse dieser Forschung für kommerzielle Zwecke durchzuführen. Weitergehende Konkretisierungen werden nicht gegeben. Bereits jetzt gibt es in der Praxis Rechtsunsicherheit darüber, wie das „primäre Ziel“ zu verstehen sein soll und welche Bemessungskriterien hierfür anzulegen sind, und ebenso, ob die Rechtsträgerschaft der Forschungseinrichtung eine Relevanz für die Einstufung von kommerziellen Zwecken besitzt. Überdies stellt sich die Frage, weshalb nicht auch Forschungseinrichtungen des Bundes in den Katalog betroffener Einrichtungen aufgenommen werden, die Cyberbedrohungen ebenso ausgesetzt sind wie mit kommerziellem Hintergrund betriebene Forschungseinrichtungen (vgl. AG KRITIS, Stel-

lungnahme zum Regierungsentwurf des NIS2UmsuCG vom 02.10.2024, S. 5, online abrufbar unter: https://ag.kritis.info/wp-content/uploads/2024/10/20241027-Stellungnahme-NIS2UmsuCG-RefE-v02102024-AG-KRITIS-v1.1.pdf).

- **§ 2 Nr. 13 BSIG-E (Begriffsbestimmungen, hier: „Geschäftsleitung“):**

Diese Vorschrift dient der Umsetzung von Art. 20 der NIS-2-Richtlinie und will die Leitungsorgane der betroffenen Einrichtungen stärker für die Cybersicherheit in die Pflicht nehmen. NIS-2 selbst spricht hier von den „Leitungsorganen wesentlicher und wichtiger“ Einrichtungen, ohne dies aber in besagtem Artikel näher zu konkretisieren. Auch die Vorschrift in § 2 Nr. 13 BSIG-E sorgt schon jetzt bei den betroffenen Unternehmen für Rechtsunsicherheit, da an die Weite bzw. Enge der Definition unmittelbare organisatorische Folgen im Unternehmen angeknüpft sind. Deshalb wäre eine inhaltliche Konkretisierung der Begriffsdefinition wünschenswert. Zurzeit wird auf die Kriterien des „Führens der Geschäfte“ und kumulativ „zur Vertretung“ der Einrichtung verwiesen, wobei sich die inhaltliche Anknüpfung aus dem Gesetz, einer Satzung oder dem Gesellschaftsvertrag ergeben kann. Jedoch ist beispielsweise auch eine einfachvertragliche bzw. arbeitsvertraglich eingeräumte Vertretungsbefugnis möglich, wie es zum Beispiel für Abteilungsleiter der Fall sein kann, die für ihren Bereich ebenso die Geschäfte führen und die Gesellschaft nach außen hin rechtswirk-

sam vertreten können – dies dürfte gerade für größere Unternehmungen mit entsprechender Abteilungsgröße relevant sein.

- **§ 2 Nr. 17 BSIG-E (Begriffsbestimmungen, hier: „Informationssicherheit“):**

  In verschiedenen anderen Stellungnahmen zum NIS2UmsuCG wird bereits auf die begrifflichen Unschärfen zu Informationssicherheit, Datensicherheit, Netzsicherheit, Netz- und Informationssicherheit, IT-Sicherheit, Cybersicherheit und Sicherheit in der Informationstechnik verwiesen (so GDD, Stellungnahme zum NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz, S. 2, online abrufbar unter: https://www.gdd.de/wp-content/uploads/2024/10/GDD-Stellungnahme-NIS2UmsuCG-mm.pdf). Richtigerweise ist hier unbedingt ein einheitliches Begriffsverständnis zu schaffen, da die vorgenannten Begriffe allesamt über eine unterschiedliche Bedeutung und Weite verfügen und daher teils nicht zum gesetzlichen Rahmen passen. Optimalerweise sollte sich der Gesetzgeber hier auf einen zentralen Begriff festlegen. Unabhängig davon ist der vorliegende Begriff der „Informationssicherheit“ auch unzureichend ausdefiniert, indem er wesentliche Schutzziele unterschlägt und nur auf die Vertraulichkeit, Integrität und Verfügbarkeit verweist. Das Kriterium der Authentizität sowie ggf. auch das Kriterium der Nichtabstreitbarkeit hingegen wird ausgeklammert.

- **§ 2 Nr. 22 BSIG-E (Begriffsbestimmungen, hier: „kritische Anlage“):**

  Der bislang geltende zentrale Begriff der „kritischen Infrastruktur“ wird künftig durch die „kritische Anlage“ ersetzt, die Bestandteil der „besonders wichtigen Einrichtungen“ ist, die von den „wichtigen Einrichtungen“ abzugrenzen sind (auf die übermäßige Komplexität dieser Begriffe und den Vorschlag zur unmittelbaren Orientierung am europäischen Rahmen nach NIS-2 wird in der im späteren Verlauf folgenden Stellungnahme zu § 28 BSIG-E verwiesen). Die Bestimmung der kritischen Anlage soll durch Rechtsverordnung erfolgen, die gegenwärtig nicht vorliegt, aber sich vermutlich künftig an den zahlenmäßigen Maßgaben der BSI-KritisV orientieren wird. Mangels weitergehender begrifflicher Konkretisierung können sich betroffene Unternehmen zurzeit deshalb noch nicht auf den neuen Anwendungsbereich vorbereiten. Hier stellt sich deshalb die Frage, ob die neue zusätzliche Kategorie der „kritischen Anlagen“ in dieser Form tatsächlich erforderlich ist, um das gesetzgeberische Ziel zu erreichen. Es bestehen schon jetzt praktische Unsicherheiten dergestalt, ob die höheren Anforderungen für die gesamte Einrichtung oder nur für den Betrieb der kritischen Anlage heranzuziehen sind. Im Sinne einer Vereinfachung der Handhabung und zur Verbesserung der Rechtssicherheit wäre deshalb anzudenken, die zusätzliche Bestimmung der „kritischen Anlage“ im Gesetzentwurf entfallen zu lassen. Die zusätzliche Kritikalität dieser Anlagen könnte hingegen bereits über die Maßnahmen des Risikomanagements Eingang in die Betrachtung finden, das ja gerade in § 30 Abs. 1 BSIG-E bereits verlangt, dass sich die zu leistenden Maß-

nahmen zum Risikomanagement u.a. am Ausmaß der Risikoexposition und den gesellschaftlichen und wirtschaftlichen Auswirkungen zu orientieren haben. Auf diese Weise könnte eine verkomplizierende Begriffsdefinition entfallen, ohne den Schutzbedarf herabzusetzen (vgl. zur Kritik der „Überkomplexität“ auch AG KRITIS, Stellungnahme zum Regierungsentwurf des NIS2UmsuCG vom 02.10.2024, S. 5, online abrufbar unter: https://ag.kritis.info/wp-content/uploads/2024/10/20241027-Stellungnahme-NIS2UmsuCG-RefE-v02102024-AG-KRITIS-v1.1.pdf). Durch eine solche Änderung würde ebenfalls die Definition der „kritischen Komponenten“ angetastet, deren Anwendungsfälle konkret untergesetzlich zu bestimmen wären, ohne auf die kritischen Anlagen Bezug zu nehmen. Generell ist in diesem übergreifenden Zusammenhang anzumerken, dass die begriffliche Unterscheidung zwischen „kritischen Anlagen“, „kritischen Komponenten“ und „kritischen Dienstleistungen“ nicht zu einer praktikableren Handhabbarkeit der Regelungen seitens betroffener Einrichtungen beiträgt.

- **§ 2 Nr. 26 BSIG-E (Begriffsbestimmungen, hier: „Managed Service Provider“):**

  Teilweise wird angemerkt, dass die Definition des „Managed Service Provider“ (MSP) zu weit gefasst ist und zahlenmäßig bzw. inhaltlich begrenzt sein sollte. Bei einem MSP handelt es sich um einen Anbieter von Diensten im Zusammenhang mit der Installation, der Verwaltung, dem Betrieb oder der Wartung von IKT-Produkten, -Netzen, -Infrastruktur, -Anwendungen oder jeglicher anderer Netz-

und Informationssysteme durch Unterstützung oder aktive Verwaltung in den Räumlichkeiten der Kunden oder aus der Ferne. Eine Eingrenzung der Begriffsdefinition sollte jedoch unabhängig von rechtlichen Fragestellungen allein schon deshalb nicht vorgenommen werden, da die MSP als Bestandteil der digitalen Lieferkette eine essenzielle Funktion auch für die Verfügbarkeit und Integrität von IT-Systemen wahrnehmen und eine Vielzahl an Unternehmen insbesondere in Deutschland derartige Leistungen anbieten und ansonsten Regelungslücken entstehen würden. Bei der Umsetzung ist dennoch darauf zu achten, dass die Vorgaben künftig im Gleichlauf mit den Anforderungen aus dem EU Cyber Resilience Act (CRA) realisiert werden, die auch auf verschiedene MSP zutreffen werden.

- **§ 2 Nr. 38 BSIG-E (Begriffsbestimmungen, hier: „Schwachstelle“):**

  Die Begriffe „Schwachstelle“ und „Sicherheitslücke“ haben grundsätzlich eine unterschiedliche Bedeutung, wie auch aus der vorgeschlagenen Gesetzesänderung hervorgeht. Die bisherige „Sicherheitslücke“ wird technisch als „Eigenschaft von Programmen oder sonstigen informationstechnischen Systemen“ beschrieben, wohingegen die „Schwachstelle“ deutlich weiter gefasst ist als eine Eigenschaft von IKT-Produkten oder IKT-Diensten, die von Dritten ausgenutzt werden kann, um sich gegen den Willen des Berechtigten Zugang zu den IKT-Produkten oder IKT-Diensten zu verschaffen oder die Funktion der IKT-Produkte oder IKT-Dienste zu beein-

flussen. Zur besseren Nachvollziehbarkeit des Handlungsrahmens im Sinne einer unabhängigen fachlich-technischen Arbeit wird empfohlen, auch in Zukunft nicht den Begriff der „Schwachstelle“, sondern denjenigen der „Sicherheitslücke“ zu verwenden. Alternativ könnte der Begriff der Sicherheitslücke beibehalten werden und die Schwachstelle als zusätzliche Definition aufgenommen werden, um anhand der jeweiligen Befugnisgrundlagen eine Abgrenzung durch Einzelverweis vorzunehmen.

- **§ 2 Nr. 11 BSIG-E (Begriffsbestimmungen, hier: „Sicherheitsvorfall“):**

  Der „Sicherheitsvorfall“ wird beschrieben als 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. Wie bereits zuvor angemerkt ist ebenfalls die Authentizität von Daten ein anerkanntes Schutzziel der Cybersicherheit und sollte deshalb ebenso in die Definition des IT-Sicherheitsvorfalls aufgenommen werden, um Regelungslücken auszuschließen.

- **§ 2 Nr. 41 BSIG-E (Begriffsbestimmungen, hier: „Systeme zur Angriffserkennung“):**

Der zwingende Einsatz von Systemen zur Angriffserkennung (SzA) ist in Fachkreisen ohnehin bereits seit Längerem umstritten, siehe dazu noch im Folgenden. Schon im geltenden Recht ist die Definition der SzA denkbar weit gefasst und auch durch die gesetzlich vorgeschlagenen Regelungen wird die neue Definition in ihrer Weite nicht eingeschränkt, indem SzA definiert werden als durch technische Werkzeuge und organisatorische Einbindung unterstützte Prozesse zur Erkennung von Angriffen auf informationstechnische Systeme, wobei die Angriffserkennung durch Abgleich der in einem informationstechnischen System verarbeiteten Daten mit Informationen und technischen Mustern, die auf Angriffe hindeuten, erfolgt. Das BSI hat die Anforderungen zum Einsatz von SzA im KRITIS-Bereich durch eine Orientierungshilfe aus dem Jahr 2022 (BSI, Orientierungshilfe zum Einsatz von Systemen zur Angriffserkennung, online abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/KRITIS/oh-sza.html) weitergehend konkretisiert. In der praktischen Umsetzung besteht dennoch weiterhin Unsicherheit darüber, ob für den Einsatz von SzA in wesentlichen und wichtigen Diensten jenseits der kritischen Infrastrukturen diese ähnlichen oder gar denselben Anforderungen genügen müssen, was sich durch eine Vielzahl am Markt verfügbarer Produkte weiter verschärft. An dieser Stelle wäre ein Verweis auf weitergehende untergesetzliche Konkretisierungen, beispielsweise durch das BSI, hilfreich bzw. alternativ eine begrifflich einengende Definition denkbar.

- **§ 3 BSIG-E (Aufgaben des Bundesamtes):**

Der Katalog der Aufgabenzuweisungen des BSI wurde in den vergangenen Jahren durch verschiedene Gesetzesnovellen laufend erweitert, damit einhergehend auch sein Ausbau als zentrale Stelle für Informationssicherheit in Deutschland. Wie bereits für den Entwurf des § 1 BSIG-E angemerkt gehen damit auch gesteigerte Erwartungen an die unabhängige und fachlich-sachliche Tätigkeit des BSI einher, die im gegenwärtigen Status des Gesetzentwurfs nicht angemessen wiedergegeben werden. Unter diesem Gesichtspunkt hervorhebenswert ist der der § 3 Abs. 18 BSIG-E. Schon nach geltendem Recht enthält diese Vorschrift die Bestimmung von Unterstützungsaufgaben des BSI gegenüber Polizeien, Strafverfolgungsbehörden und Nachrichtendienstbehörden. Daraus geht jedoch noch nicht ausreichend eindeutig hervor, auf welchem Wege die Unterstützungsleistung erfolgt, welche Ziele sie bezweckt und welchen Einschränkungen sie zu genügen hat. Im Zweifelsfall ist nach gegenwärtigem Stand nicht eindeutig aus der gesetzlichen Formulierung heraus klärbar, worin die „gesetzlichen Aufgaben“ von Sicherheitsbehörden bestehen sollen, bei denen das BSI Unterstützungsleistungen erbringt. So können gesetzliche Aufgaben auch solche sein, die die IT-Sicherheit schwächen, indem beispielsweise Maßnahmen nach der StPO zur Durchführung von Quellen-Telekommunikationsüberwachungen oder Online-Durchsuchungen durchgeführt werden – für die das BSI weder zuständig ist noch als Cybersicherheitsbehörde irgendwie geartete Unterstützung leisten darf. Deshalb sollten diese Aufgaben schon hier weitergehend konkretisiert werden bzw. zumindest festgestellt werden, dass diese Unterstützungsleistungen nicht zu einer

Schwächung der Cybersicherheit, sondern zu ihrer Stärkung führen müssen, indem beispielsweise Unterstützung bei der Aufklärung von Cyberkriminalität geleistet wird. Überdies mutet die bereits geltende – und durch NIS2UmsuCG nur geringfügig angetastete – Ausnahmeregelung unter diesem Gesichtspunkt eigentümlich an, schlägt sie in § 3 Nr. 18 lit. c) BSIG-E doch vor, dass die Unterstützung auch gewährt werden darf, soweit sie erforderlich ist, um Tätigkeiten zu verhindern oder zu erforschen, die „unter Nutzung der Informationstechnik erfolgen“. Es ist dringend anzuraten, diesen zweiten Halbsatz zu streichen, um einer Ausweitung der Unterstützungsleistungen gegen die Ziele der Informationssicherheit unter dem Dach der Aufgabenzuweisungen des BSI entgegenzuwirken (so richtigerweise auch GDD, Stellungnahme zum NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz, S. 2 f., online abrufbar unter: https://www.gdd.de/wp-content/uploads/2024/10/GDD-Stellungnahme-NIS2UmsuCG-mm.pdf).

Gemäß der Verordnung (EU) 2022/2554 über die digitale operationale Resilienz im Finanzsektor (DORA) gelten spezielle Anforderungen für die Informationssicherheit im hochregulierten Bereich der Finanzunternehmen. § 3 Nr. 29 BSIG-E schreibt deshalb richtigerweise vor, dass das BSI mit der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) zur Aufgabenerfüllung kooperiert und Informationen austauscht, soweit dies zur Aufgabenerfüllung erforderlich ist. Diese Formulierung ist jedoch nicht weitreichend genug, da schon jetzt in der Umsetzungspraxis der europäischen und nationalen Regulierung zur Informationssicherheit Abgren-

zungsschwierigkeiten zwischen den Tätigkeiten von BSI und BaFin, bestehen, die bei den betroffenen Unternehmen zu Mehraufwänden und vor allem zu Rechtsunsicherheit über Zuständigkeiten führen. § 3 Nr. 29 BSIG-E sollte daher um eine Vorgabe ergänzt werden, dass nicht nur Kooperation und Informationsaustausch stattfinden, sondern eine Abstimmung und Klärung eventueller Zuständigkeitsüberschneidungen stattfindet, die durch die regulierten Finanzunternehmen an BSI und BaFin herangetragen werden.

- **§ 5 BSIG-E (Allgemeine Meldestelle für die Sicherheit in der Informationstechnik):**

  Infolge des bereits für § 3 BSIG-E skizzierten zunehmenden Ausbaus des BSI als zentrale Stelle für Informationssicherheit in Deutschland geht eine erheblich gesteigerte Verantwortung für den Umgang mit den erlangten, teils hochsensiblen und unter Umständen auch geschäftsgeheimnisbezogenen Daten einher. Nur wo ein Vertrauen in die behördlichen Strukturen zur Informationssicherheit in Deutschland herrscht, kann auch eine funktionierte nationale digitale Sicherheitsarchitektur aufgebaut werden. Auf die mit der fehlenden institutionellen Unabhängigkeit des BSI einhergehenden Probleme wurde in dieser Stellungnahme bereits u.a. unter § 1 BSIG-E eingegangen. Hervorzuheben sei an dieser Stelle jedoch erneut, dass das BSI mangels institutioneller Unabhängigkeit nach wie vor dem Geschäftsbereich des Bundesministeriums des Innern und für Heimat (BMI) zuzuordnen ist, dem auch Polizei- und Nachrichtendienstbehörden unterfallen. Deshalb scheint hier gem. § 5

Abs. 3 BSIG-E eine eindeutige Klarstellung dergestalt geboten, dass die gemeldeten Informationen ausschließlich zur Verbesserung der Informationssicherheit verwendet und weitergegeben werden dürfen und eine Verwendung und Weitergabe der Informationen zur Ausnutzung von ebenjenen festgestellten oder gemeldeten Sicherheitslücken bzw. Schwachstellen nicht stattfindet. Abweichungen vom in der Vorschrift gegenwärtig wiedergegebenen intendierten Ermessen, eine Information zu Zwecken der Verbesserung der Informationssicherheit weiterzugeben, müssen auf absolute Ausnahmefälle beschränkt sein, sind zu dokumentieren und einzelfallbezogen zu begründen und dürfen nicht ausschließlich auf eine Weisung aus dem BMI zurückzuführen sein, ggf. ist hier zusätzlich ein abschließender Katalog berechtigter bzw. widerstreitender Interessenspositionen zu nennen, die denen der Informationssicherheit in einer verfassungsrechtlichen Abwägung ebenbürtig sind (vgl. auch Claudia Plattner, Präsidentin des BSI, Stellungnahme zur öffentlichen Anhörung des Innenausschusses des Deutschen Bundestags am 4. November 2024, S. 14, online abrufbar unter: https://www.bundestag.de/ausschuesse/a04_inneres/anhoerungen/1026172-1026172).

- **§ 6 BSIG-E (Informationsaustausch):**

Die Einrichtung einer Online-Plattform zum Informationsaustausch über Cyberbedrohungen, Schwachstellen, Beinahevorfälle und IT-Sicherheitsmaßnahmen sowie zur Aufdeckung und Abwehr von

Cyberangriffen (Information Sharing Portal) ist zu begrüßen, da sie zu einer deutlich verbesserten Aufbereitung, verlässlichen Quelle und schnellen Verteilung cybersicherheitsrelevanter Informationen führt. Hier sollte jedoch von Anfang an sichergestellt werden, dass alle relevanten behördlichen Akteure eingebunden werden, indem ein ganzheitlicher Ansatz verfolgt wird, der nicht nur die Informationssicherheit, sondern ebenso die hybride Bedrohungslage adressiert, beispielsweise Gefährdungen durch Sabotage oder Desinformation. Hilfreich wäre überdies die Integration von zielgruppengerechten Handlungsempfehlungen und Unterstützungsangeboten in das Information Sharing Portal. In den Prozess der Erarbeitung der Teilnahmebedingungen und Aufbau der Plattform sollten deshalb zu bestmöglicher Effizienz und Effektivität der Plattform Verbände und relevante Wirtschaftsakteure von Anfang an einbezogen werden.

- **§ 7 BSIG-E (Kontrolle der Kommunikationstechnik des Bundes, Betretensrechte):**

  Gem. § 7 Abs. 1 BSIG-E ist das BSI befugt, die Sicherheit der Kommunikationstechnik des Bundes und ihrer Komponenten, einschließlich technischer Infrastrukturen, die zum Betrieb der Kommunikationstechnik des Bundes erforderlich sind, zu kontrollieren. Gemäß den Absätzen 6 und 7 (und an weiteren Stellen im BSIG-E die Sicherheit der Kommunikationstechnik des Bundes betreffend) werden hiervon aber umfassende Ausnahmetatbestände vorgesehen, so für das Auswärtige Amt, die Streitkräfte und den Militäri-

schen Abschirmdienst, ohne dass erkennbar wäre, wie für diese Einrichtungen auf alternativem Wege vergleichbare Kontrollmechanismen vorgesehen wären. Im Sinne eines einheitlichen Niveaus der Informationssicherheit in der deutschen Verwaltung ist zu empfehlen, diese Ausnahmen zu streichen – unabhängig von den gegebenen europarechtlichen Möglichkeiten.

§ 7 Abs. 8 BSIG-E bestimmt überdies, dass wenn das BSI im Rahmen seiner Kontrollen feststellt, dass ein Verstoß gegen die Verpflichtungen des BSIG eine offensichtliche Datenschutzverletzung zur Folge hat, die gem. Art. 33 DS-GVO meldepflichtig ist, es unverzüglich die zuständigen Aufsichtsbehörden hierüber unterrichtet. Unklar ist, warum sich diese Vorschrift zur Weitergabe ausschließlich auf „offensichtliche Datenschutzverletzungen“ beschränkt, obwohl der europarechtliche Rahmen an dieser Stelle deutlich enger gefasst ist. Hier sollte eine Weitergabe bereits bei der „bloßen Möglichkeit“ der Datenschutzverletzung erfolgen.

- **§ 28 BSIG-E (Besonders wichtige und wichtige Einrichtungen):**

Nach wie vor erschließt sich nicht, weshalb der deutsche Gesetzgeber nicht die europäischen Begrifflichkeiten in der Unterscheidung zwischen „wesentlichen“ und „wichtigen“ Einrichtungen übernimmt und anstelle dessen mit den „besonders wichtigen“ und den „wichtigen“ Einrichtungen neue Alternativbegriffe einführt, die Rechtsunsicherheit stiften. Auch die zusätzliche neue Subkategorie der „Betreiber kritischer Anlagen“ ist wie zuvor dargestellt nicht

zwingend notwendig, um dem gesteigerten Schutzbedarf dieser durch das Gesetz adressierten Einrichtungen auf angemessene Weise gerecht zu werden.

An verschiedenen Stellen hat es in der Vergangenheit Kritik an der tatbestandlichen Weite der durch NIS-2 und damit auch NIS2UmsuCG zusätzlich adressierten Unternehmen gegeben. Dazu ist festzustellen: Weder an der europäischen Size-Cap-Rule in quantitativer Hinsicht noch qualitativ mit Blick auf die sektoralen Zugehörigkeiten lassen sich im bundesdeutschen Recht deutliche Anpassungen vornehmen, ohne gegen die Vorgaben des Europarechts zu verstoßen. Der tatsächliche rechtliche Gestaltungsspielraum des deutschen Gesetzgebers ist hier limitiert. Die Frage der Umsetzung und Überprüfbarkeit von ca. 30.000-40.000 durch NIS-2 betroffenen Unternehmen ist davon losgelöst zu sehen und betrifft erst einmal nicht das in Rede stehende Gesetzgebungsverfahren zu NIS2UmsuCG, sondern dessen spätere Umsetzung.

- **§ 29 BSIG-E (Einrichtungen der Bundesverwaltung):**

Im Hinblick auf die Risiken eines Abfalls des Informationssicherheitsniveaus von Einrichtungen der Bundesverwaltung im Vergleich zu privatwirtschaftlichen Akteuren wird auf die umfassende Kritik verwiesen, die bereits in verschiedenen anderen Stellungnahmen adressiert wurde (so z.B. auch AG KRITIS, Stellungnahme zum Regierungsentwurf des NIS2UmsuCG vom 02.10.2024, S. 6 ff. online abrufbar unter: https://ag.kritis.info/wp-

content/uploads/2024/10/20241027-Stellungnahme-NIS2UmsuCG-RefE-v02102024-AG-KRITIS-v1.1.pdf; Prof. Timo Kob, Stellungnahme NIS2UmsuCG, S. 3 ff., online abrufbar unter: https://www.bundestag.de/resource/blob/1027134/727dccd4a80e3a14cfdce9d59a1fab38/20-4-523-A.pdf; GDD, Stellungnahme zum NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz, S. 4, online abrufbar unter: https://www.gdd.de/wp-content/uploads/2024/10/GDD-Stellungnahme-NIS2UmsuCG-mm.pdf). Bei der Bewertung der Bedrohungslage in der Informationssicherheit kann nicht derart deutlich zwischen staatlichen und nichtstaatlichen Akteuren unterschieden werden, sondern alle Einrichtungen sind gleichermaßen erfasst – man wird im Gegenteil sogar davon auszugehen haben, dass in Zeiten der hybriden Bedrohungslage und von Cyberwarfare und internationalen Spionageaktivitäten staatliche Einrichtungen noch stärker im Fokus stehen als manches mittelständische Unternehmen, das neuerdings ebenso in den Anwendungsbereich von NIS-2 fällt. Gleichwohl ist es jedoch nicht so – wie teils auch suggeriert wird – dass Einrichtungen der Bundesverwaltung kaum oder gar keine Informationssicherheit umzusetzen haben, da sich in den §§ 43 ff. BSIG-E Spezialregelungen zu diesem Themenkomplex finden, auf die noch im Folgenden eingegangen wird. Dennoch sollte unter Berücksichtigung vorgenannter Kritik berücksichtigt werden, dass trotz der Ausnahmetatbestände im Endeffekt ein Informationssicherheitsniveau realisiert werden sollte, das demjenigen der privatwirtschaftlich betroffenen Einrichtungen mindestens ebenbürtig ist. Unter diesem Gesichtspunkt ist auch die Regelung des § 37 BSIG-E (Ausnahmebescheid) zu sehen, denn europarechtlich kann zwar

vorgesehen sein, dass bestimmte öffentliche Bereiche von der Regulierungshoheit auch nach NIS-2 ausgenommen sind, ob diese rechtliche Konsequenz jedoch auch zwingend in das nationale Recht übertragen werden muss, kann man durchaus hinterfragen, denn die Informationssicherheit sollte vielleicht gerade in diesen sicherheitssensiblen Bereichen mit einem höchstmöglichen Standard gewährleistet werden.

Unter rechtssystematischen Gesichtspunkten ist die Regelung des § 29 BSIG-E ungünstig, da sie im Zusammenhang mit den §§ 43 ff. BSIG-E zu sehen ist. Zu empfehlen wäre deshalb, die Definition der „Einrichtungen der Bundesverwaltung“ aus § 29 Abs. 1 BSIG in die Begriffsbestimmungen gem. § 2 BSIG-E zu übertragen, damit sie an späterer Stelle wiederverwendet werden kann und eine systematische Verbindung über das gesamte Gesetz hinweg zwischen § 29 BSIG-E und §§ 43 ff. BSIG-E hergestellt werden kann. Auch dürfte ein unmittelbar in § 29 BSIG-E enthaltener Verweis sinnvoll sein, dass trotz der Ausnahmetatbestände in den §§ 43 ff. BSIG-E eigenständige Regelungen für die Informationssicherheit in der Bundesverwaltung vorgesehen sind.

- **§ 30 BSIG-E (Risikomanagementmaßnahmen besonders wichtiger Einrichtungen und wichtiger Einrichtungen):**

  § 30 BSIG-E enthält mit der Festlegung der Risikomanagementmaßnahmen von besonders wichtigen und wichtigen Einrichtungen ein Kernelement der nationalen Umsetzung von NIS-2. Wenngleich

die nationalen Umsetzungsspielräume infolge der sehr konkreten Regelung aus Art. 21 NIS-2 nur begrenzt sind, sind Verbesserungen an dieser Stelle angeraten. Dies betrifft insbesondere die unmittelbare Übernahme des europarechtlich vorgegebenen Maßnahmenkatalogs in § 30 Abs. 2 BSIG, der im Sinne eines Mindestkatalogs diejenigen Maßnahmen zur Informationssicherheit beschreibt, die in jedem Falle minimal umzusetzen sind. Dieser aus dem europäischen Recht kommende Katalog ist nicht nur irreführend, sondern auch unpraktikabel, indem er einzelne Maßnahmen in den Vordergrund stellt, die teils noch nicht einmal auf jedes durch NIS-2 betroffene Unternehmen anwendbar sind. Überdies suggeriert er, durch einzelne Produkte eine NIS-2-Konformität herstellen zu können, wo es eigentlich doch auf die Etablierung eines fortlaufenden Risikomanagementsystems zur Informationssicherheit ankommt. Empfohlen wird deshalb, auf die Übernahme dieses Katalogs zu verzichten und im Wege einer „unionsrechtskonformen Auslegung“ auf die Umsetzung von Risikomanagement nach Stand der Technik gem. § 30 Abs. 1 BSIG-E zu verweisen. Dies würde vielen betroffenen Einrichtungen nicht nur die Umsetzung erleichtern, sondern auch nicht unbedingt nötige Mehraufwände bei der Umsetzung vermeiden. Dass dies realisierbar ist, belegt die Umsetzung im mitgliedstaatlichen Vergleich, wo teils zwar inhaltliche Übernahmen des Katalogs stattfinden, teils aber auch kein Bezug auf den Katalog genommen und beispielsweise auf untergesetzliche Konkretisierungen verwiesen wird. Der verwendete Maßnahmenkatalog nach NIS-2 ist überdies auch zu unbestimmt – so werden Begriffe wie „Cyberhygiene“ aufgelistet, ohne zu definieren, was hierunter zu verstehen ist und inwieweit sich die damit ver-

bundenen Maßnahmen zur Informationssicherheit von den bereits beschriebenen anderen Maßnahmen unterscheiden. Überdies stellt sich die Frage, ob nicht auch jenseits der besonders wichtigen Einrichtungen Branchenverbände an der Erarbeitung eigener und bereichsspezifischer Standards zur Informationssicherheit mitwirken können sollten, die mit dem BSI abgestimmt werden.

Kritisch zu würdigen ist ebenfalls der § 30 Abs. 6 BSIG-E, der vorschreibt, dass besonders wichtige Einrichtungen und wichtige Einrichtungen durch Rechtsverordnung nach § 56 Abs. 3 bestimmte IKT-Produkte, IKT-Dienste und IKT-Prozesse nur verwenden dürfen, wenn diese über eine Cybersicherheitszertifizierung gem. europäischer Schemata nach Art. 49 der Verordnung (EU) 2019/881 (Cybersecurity Act) verfügen. Fraglich ist an dieser Stelle, weshalb eine ausschließliche Bezugnahme auf das CSA-Framework stattfindet, wenn anstelle dessen grds. mehrere Optionen zur Verfügung stehen, um ein Risikomanagement nach NIS-2 durchzuführen und nachzuweisen. Hinzu tritt an dieser Stelle, dass sich die Cybersecurity Certification Schemes nach CSA bereits seit Jahren in der Erstellung befinden, insbesondere mit Blick auf Schlüsseltechnologien wie Cloud und 5G und somit zumindest zurzeit keine verlässliche Nachweisgrundlage darstellen können.

- **§ 31 BSIG-E (Besondere Anforderungen an die Risikomanagementmaßnahmen von Betreibern kritischer Anlagen):**

Wie bereits dargelegt stellt sich die Frage, ob neben den wesentlichen Einrichtungen nach NIS-2 eine weitere Kategorie von betroffenen Einrichtungen in Form der Betreiber kritischer Anlagen benötigt wird – dies ist nur dann der Fall, wenn ohne eine solche Regelung Schutzlücken in der Informationssicherheit bestünden. Da § 30 BSIG-E zur Bewertung des Informationssicherheitsniveaus bereits an eine individuelle Risikoanalyse eines Unternehmens anknüpft, können hierüber bereits solche betroffenen Einrichtungen mit einer höheren Risikoprävalenz abgedeckt werden. Insoweit enthält auch der § 31 Abs. 1 BSIG-E keine nennenswerten inhaltlichen Erkenntnisse, die über die Regelung in § 30 Abs. 1 BSIG-E hinausgingen.

Überdies wurde auch die Verpflichtung zum Einsatz von Systemen zur Angriffserkennung (SzA) für die Betreiber kritischer Anlagen in der Vergangenheit mehrfach kritisiert. Dies einerseits aus europarechtlichen Gründen, weil diese starre Festlegung nicht mit den technischen Zielen aus der jüngst veröffentlichten Durchführungsverordnung (EU) 2024/2690 korreliert, andererseits aber auch aus technischen Gründen, weil nicht klar ist, warum SzA gegenüber anderen Maßnahmen, die im Rahmen eines Risikomanagements nach NIS-2 zu ergreifen sein können, eine besonders herausgehobene Stellung genießen sollten, zumal der Aufbau und Betrieb von SzA mit erheblichen wirtschaftlichen Aufwänden verbunden sein kann.

- **§ 32 BSIG-E (Meldepflichten):**

Grundsätzlich ist zu begrüßen, dass nach NIS-2 ein mehrstufiges Meldeverfahren vorgesehen ist, das an den unterschiedlichen Informations- und Kenntnisstand der betroffenen Einrichtungen zum jeweiligen Zeitpunkt anknüpft. Auch hier sollte jedoch ein Augenmerk darauf gelegt werden, das Meldeverfahren möglichst unbürokratisch zu gestalten und Mehraufwände durch Mehrfachmeldungen zu vermeiden. Der mit der Vorschrift nunmehr verfolgte Ansatz, einen Gleichlauf zwischen KRITIS-DachG und NIS2UmsuCG herzustellen, indem eine gemeinsame Meldestelle geschaffen wird, ist deshalb begrüßenswert. Darüber hinaus sind jedoch im Bereich der Informationssicherheit in Deutschland weitere Behörden eingebunden, so u.a. die Bundesnetzagentur (BNetzA) und die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin). Wie ebenfalls in dieser Stellungnahme bereits dargelegt kann mit einer Verletzung der Informationssicherheit zugleich auch eine Datenschutzverletzung nach DS-GVO einhergehen, die zusätzliche Meldepflichten auslöst. Hier ist es den betroffenen Unternehmen nicht mehr zumutbar, zahlreiche verschiedene Meldekanäle mit unterschiedlichen formalen Anforderungen an die Meldung gleichzeitig zu bespielen und zu ermitteln, welcher Meldekanal auf welcher Rechtsgrundlage für den Einzelfall einschlägig ist. Daher ist anzuraten, die Zentralisierung einer gemeinsamen Meldestelle weiter auszudehnen und weitere Behörden und ggf. die Datenschutzaufsicht einzubeziehen, sodass die Meldung ohne Zutun der betroffenen Einrichtung stets an die zuständigen Stellen weitergegeben wird. Hierdurch wird nicht nur die Akzeptanz der Meldepflicht verbessert, sondern auch ein höheres Informationssicherheitsniveau

insgesamt erzielt, da die Meldungen stets an der richtigen Stelle zeitnah ankommen. Überdies sind in der nationalstaatlichen Umsetzung in europäischer Koordination Maßnahmen zu bestimmen, wie insbesondere bei multinationalen Unternehmen, die in mehreren EU-Mitgliedstaaten gleichzeitig tätig sind, ggf. Meldewege erleichtert werden können.

- **§ 33 BSIG-E (Registrierungspflicht):**

Besonders wichtige und wichtige Einrichtungen sowie Domain-Name-Registry-Diensteanbieter sind verpflichtet, sich gem. § 33 Abs. 1 BSIG-E spätestens nach drei Monaten bei einer gemeinsamen Registrierungsmöglichkeit von BSI und BBK zu registrieren und die in der Vorschrift bestimmten Angaben zu übermitteln. Nach gegenwärtigem Stand herrscht bei den (potenziell) durch NIS-2 betroffenen Unternehmen nach wie vor eine erhebliche Rechtsunsicherheit hinsichtlich der eigenen Betroffenheit. Zwar obliegt den betroffenen Einrichtungen selbst die Prüfpflicht, ob sie von bestimmten Regularien aufgrund des Vorliegens der tatbestandlichen Voraussetzungen betroffen sind, jedoch erscheint es sinnvoll, seitens des BSI eine bestmögliche Unterstützung bei der Identifikation der eigenen Betroffenheit anzubieten. Einige Ansätze werden in verschiedenen öffentlichen Stellungnahmen diskutiert, wenngleich diese sicherlich noch nicht ausgereift sind (so zum Beispiel Deutsche Industrie- und Handelskammer, Stellungnahme zum Entwurf von NIS2UmsuCG, S. 9 f., online abrufbar unter: https://www.dihk.de/resource/blob/117740/ff85113d4d8e5ff606301f

57a3aeecdd/recht-dihk-stellungnahme-umsetzungs-und-cybersicherheitsstaerkungsgesetz-data.pdf). Denkbar wäre darüber hinaus auch eine Rückmeldung des BSI bei registrierten Unternehmen nach Registrierungseingang, sollten diese nicht vom Anwendungsbereich von NIS2UmsuCG betroffen sein und sollte insoweit eine juristische Fehleinschätzung vorliegen.

- **§ 38 BSIG-E (Umsetzungs-, Überwachungs- und Schulungspflicht für Geschäftsleitungen besonders wichtiger Einrichtungen und wichtiger Einrichtungen):**

  Grundsätzlich ist es begrüßenswert, dass die Pflicht zur Informationssicherheit auch als Bestandteil einer ordnungsgemäßen Geschäftsorganisation benannt wird, um ihre Relevanz zu herauszustellen. Insoweit ist auch nicht den teilweise vertretenen Auffassungen zu folgen, dass sich diese Gewährleistungsverantwortung bereits aus dem allgemeinen Gesellschaftsrecht ergäbe – denn ansonsten wäre es auch nicht notwendig, die Informationssicherheit speziell zu regulieren, weil sich diese ebenfalls als Maßgabe aus der allgemeinen Pflicht zur ordnungsmäßigen Geschäftsleitung z.B. nach GmbHG oder AktG ableiten könnte.

  Dennoch ist die Vorschrift in ihrer gegenwärtigen Fassung noch zu unbestimmt, dies betrifft neben der Definition des Begriffs „Geschäftsleitung“ wie eingangs dargestellt insbesondere die Schulungspflichten gem. § 38 Abs. 3 BSIG-E. Gegenwärtig müssen Geschäftsleitungen regelmäßig an Schulungen teilnehmen, um aus-

reichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken und Risikomanagementpraktiken im Bereich der Informationssicherheit zu erlangen und dies beurteilen zu können. Es wird jedoch nicht konkretisiert, welchen Umfang solche Schulungen haben müssen, ob mit der Schulung entsprechende Nachweise zu erbringen sind und was die „Regelmäßigkeit“ bedeutet. Dies ist einerseits unter dem Gesichtspunkt der Informationssicherheit selbst verbesserungswürdig, andererseits aber auch deshalb, weil für die betroffenen Geschäftsleiter selbst unklar ist, ab welchem Zeitpunkt und in welcher Regelmäßigkeit sie ihre gesetzlichen Pflichten erfüllt haben.

- **§ 39 BSIG-E (Nachweispflichten für Betreiber kritischer Anlagen):**

  Gemäß dieser Vorschrift haben die Betreiber von kritischen Anlagen die Umsetzung der Informationssicherheitsmaßnahmen alle drei Jahre gegenüber dem BSI nachzuweisen. Auf den Begriff und die Notwendigkeit des Betreibers einer kritischen Anlage wurde bereits in anderen Teilen dieser Stellungnahme eingegangen. Für die besonders wichtigen Einrichtungen räumt das BSIG in § 61 BSIG-E jedoch bereits umfassende Aufsichts- und Durchsetzungsmaßnahmen ein. Deshalb stellt sich die Frage, inwieweit die dreijährige Nachweispflicht darüber hinausgehend noch nennenswerte Vorteile bringt bzw. ob durch sie bestimmte wirtschaftliche und personelle Kapazitäten in der Informationssicherheit nicht eher gebunden als gefördert werden.

Unabhängig hiervon sollte angedacht werden, die Anforderungen an Dokumentation und Nachweis auch jenseits der Betreiber kritischer Anlagen im Allgemeinen für besonders wichtige und wichtige Einrichtungen nach NIS2UmsuCG gesetzlich weiter zu konkretisieren, da die Ausgestaltung dieser Anforderungen aktuell in der Praxis ebenfalls noch mit erheblichen Unsicherheiten verbunden ist.

- **§ 43 BSIG-E (Informationssicherheitsmanagement):**

Die Vorschrift konkretisiert die Anforderungen an das Informationssicherheitsmanagement in der Bundesverwaltung. Auf die in diesem Zusammenhang bestehenden rechtssystematischen Schwächen wurde in dieser Stellungnahme bereits im Vorfeld im Rahmen des § 29 BSIG-E eingegangen – durch eine fehlende Bezugnahme steht das gesamte Kapitel 3 des BSIG-E mehr oder weniger „mitten im Raum“.

Wo auf der einen Seite ein möglichst umfassendes Lagebild zur Informationssicherheit in Deutschland aufgebaut werden soll, müssen auf der anderen Seite auch möglichst umfassende Informationsgrundlagen zur Verfügung stehen. Im öffentlichen Bereich bezieht dies alle Behörden ein, deren Aufgabenbereich unmittelbar oder mittelbar durch Fragen der Informationssicherheit tangiert ist. An dieser Stelle sieht § 43 Abs. 5 S. 4 BSIG-E eine deutliche Privilegierung von Bundesnachrichtendienst (BND) und Bundesamt für Verfassungsschutz (BfV) vor, indem diese von den gesetzlich angeordneten Meldepflichten explizit ausgenommen werden. Diese

Privilegierung sollte gestrichen werden, da sie nicht im Sinne einer Verbesserung der Informationssicherheit ist und die in die Abwägung einzubeziehenden Geheimschutzinteressen an dieser Stelle nicht das Interesse an mehr Informationssicherheit überwiegen.

- **§ 44 BSIG-E (Vorgaben des Bundesamtes):**

§ 44 BSIG-E bestimmt in Abs. 1, dass die Einrichtungen der Bundesverwaltung die jeweils geltenden Fassungen der Mindeststandards für die Sicherheit in der Informationstechnik des Bundes erfüllen müssen. Abs. 2 bestimmt, dass das Bundeskanzleramt und die Bundesministerien als zusätzliche Mindestanforderungen die BSI-Standards und das IT-Grundschutz-Kompendium des BSI in der jeweils geltenden Fassung einhalten müssen. Beide Regelungen sind jedoch am Ende des jeweiligen Absatzes mit einer Ausnahme dergestalt versehen, dass die Ausnahmen nach § 7 Abs. 6 und 7 BSIG-E entsprechend gelten. Diese Vorschriften wiederum enthalten umfangreiche Ausnahmetatbestände betreffend die Auslandsinformations- und -kommunikationstechnik nach § 9 Abs. 2 des Gesetzes über den Auswärtigen Dienst sowie für die Informations- und Kommunikationstechnik, die von den Streitkräften für ihre Zwecke oder dem Militärischen Abschirmdienst im Geschäftsbereich des Bundesministeriums der Verteidigung genutzt wird. Gerade für diese genannten Fälle sollte Informationssicherheit eigentlich eine herausgehobene Rolle spielen, da nicht nur sicherheitssensitive Bereiche betroffen sind, sondern unter Umständen auch geheimschutzrelevante Daten verarbeitet werden. Daher ist es an

dieser Stelle nicht empfehlenswert, durch entsprechende Ausnahmetatbestände das Mindestniveau der Informationssicherheit herabzusetzen.

Ein vergleichbarer Ausnahmetatbestand findet sich in der Vorgabe nach § 44 Abs. 6 S. 3 BSIG-E, der die grundlegende Verpflichtung von Einrichtungen der Bundesverwaltung bestimmt, IT-Sicherheitsprodukte beim BSI abzurufen. Hiervon ausgenommen werden die in § 2 Nr. 21 BSIG-E genannten Gerichte und Verfassungsorgane sowie die Auslandsinformations- und -kommunikationstechnik gem. § 7 Abs. 6 BSIG-E.

- **§ 48 BSIG-E (Amt des Koordinators für Informationssicherheit):**

  § 48 BSIG-E legt fest, dass die Bundesregierung eine Koordinatorin oder einen Koordinator für Informationssicherheit bestellt. Diese Bestimmung ist dem Grunde nach begrüßenswert, jedoch fehlt es an einer konkretisierenden inhaltlichen Ausgestaltung, welche Anforderungen und Befugnisse mit dem Amt verbunden sind und wo dieses strukturell anzusiedeln ist. Ein Koordinator für Informationssicherheit bzw. CISO Bund wird nur dann effektiv arbeiten können und seiner Aufgabenbestimmung hinreichend gerecht, wenn er entsprechende Durchsetzungsbefugnisse erhält, sein Tätigkeithorizont klar umschrieben ist und er hinreichend unabhängig im nationalen Verwaltungsgefüge angesiedelt wird und entsprechend agieren kann. Hierzu liegen bereits verschiedene öffentliche Vor-

schläge vor, unter anderem auch in den Stellungnahmen zu NIS2UmsuCG (u.a. Claudia Plattner, Präsidentin des BSI, Stellungnahme zur öffentlichen Anhörung des Innenausschusses des Deutschen Bundestags am 4. November 2024, S. 2. f. online abrufbar unter: https://www.bundestag.de/ausschuesse/a04_inneres/anhoerungen/1026172-1026172). Insgesamt wird es für die Frage der Verortung des Amts des Koordinators für Informationssicherheit in entscheidendem Maße darauf ankommen, wie unabhängig das BSI tatsächlich ist bzw. sein wird. Eine Stabsstelle jedoch, die weder mit ausreichenden Befugnissen ausgestattet ist noch eine hinreichende Unabhängigkeit besitzt, wird den Anforderungen an das Amt eines Koordinators für Informationssicherheit kaum gerecht werden können. Insoweit ist eine dringende inhaltliche Konkretisierung des § 48 BSIG-E geboten, um das Amt künftig mit Leben zu füllen.

Bremen, den 31. Oktober 2024

Prof. Dr. jur. Dennis-Kenji Kipker

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
20(4)523 H

Stellungnahme zum Entwurf des NIS2-Umsetzungsgesetzes

Prof. Dr. Haya Schulmann
ATHENE Nationales Forschungszentrum für angewandte Cybersicherheit &
Institut für Informatik, Goethe-Universität Frankfurt am Main

1. November 2024

Vorbemerkung

Im Folgenden beziehen wir uns auf den "Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung", Bundestagsdrucksache 20/13184 vom 02.10.2024, kurz: NIS-2-Umsetzungsgesetz. Verweise auf bestimmte Paragraphen beziehen sich jeweils auf Artikel 1 des NIS2-Umsetzungsgesetzes, also die Neufassung des BSI-Gesetzes.

Die Digitalisierung von Staat, Wirtschaft und Gesellschaft schreitet rasant voran, in Deutschland und weltweit. Im internationalen Vergleich belegt Deutschland in der Digitalisierung allerdings nur mittlere Plätze, und das gilt gleichermaßen für Wirtschaft und Verwaltung.[1] Gleichzeitig herrscht Einigkeit, dass eine beschleunigte und bessere Digitalisierung eine Voraussetzung für die Wahrung unseres Wohlstands und die Ankurbelung des Wachstums in Deutschland und Europa insgesamt ist.

Digitalisierung, Cybersicherheit und der Schutz der Privatsphäre sind eng miteinander verwoben. Digitalisierung ohne ausreichenden Schutz vor Cyberangriffen und Datenschutzverletzungen ist offensichtlich unverantwortlich. Umgekehrt profitieren Cybersicherheit und Privatsphärenschutz von einer umfassenden Digitalisierung, da hierdurch manuelle Eingriffe und Medienbrüche, also typische Angriffspunkte vermieden werden.

Statistiken wie die im Gesetzesentwurf zitierte BITKOM-Umfrage zu den jährlichen Schäden für die deutsche Wirtschaft durch Cyber-Ereignisse belegen eindrücklich die Größe des Cyber-Sicherheitsproblems. Die BITKOM-Umfrage vom August 2024 ergab einen geschätzten Schaden von ca. 266 Mrd. Euro – das entspräche als Summe fast 60% des Bundeshaushalts für 2024. Nicht enthalten in dieser Statistik sind die Schäden für

[1] Digitalisierung der Wirtschaft in Deutschland – Digitalisierungsindex 2023; BMWK, Berlin 2024
https://www.de.digital/DIGITAL/Redaktion/DE/Digitalisierungsindex/Publikationen/publikation-digitalisierungsindex-2023-kurzfassung.pdf?__blob=publicationFile&v=3

Staat und Verwaltungen, Hochschulen und Forschungseinrichtungen, Vereine und Stiftungen, politische Parteien und direkt für Bürgerinnen und Bürger. Auch unsere eigenen Studien in ATHENE zur Verwundbarkeit der IT-Infrastrukturen einzelner Organisationen und Sektoren (z.B. politische Parteien, Landesverwaltungen, Forschungseinrichtungen und Universitäten, Großunternehme, Medien) bestätigen die insgesamt sehr hohe Verwundbarkeit und damit den dringenden Handlungsbedarf.

Die Zunahme der Risiken im Cyberraum ist eine unvermeidliche Begleiterscheinung der Erfolge in der Digitalisierung und des Fortschritts in der IT, insbesondere in der künstlichen Intelligenz. Zusätzlich wirken sich die zunehmenden geopolitischen Spannungen auch auf den Cyberraum aus, insbesondere die Spannungen mit Russland, China, Iran und den jeweiligen Verbündeten. Alle drei sind sehr aktiv im Bereich von Cyberangriffen, Desinformation und kognitiver Kriegführung und tragen wesentlich zur angespannten Cybersicherheitslage in Deutschland bei.[2]

Es ist deshalb sehr zu begrüßen, dass sich die EU zunehmend im Bereich der Cybersicherheit engagiert und eine Anhebung des Cyber-Sicherheitsniveaus in Europa und eine Harmonisierung und Vereinheitlichung in den Mitgliedsstaaten anstrebt. Die NIS2-Richtlinie der EU (2022/2555) und das deutsche NIS2-Umsetzungsgesetz gehen zweifellos in die richtige Richtung. Im Detail sehen wir allerdings in einigen Bereichen einen Verbesserungs- oder Ergänzungsbedarf, den wir in den folgenden sechs Empfehlungen zusammenfassen.

Empfehlung 1:
Einheitlichkeit über Sektoren und Ebenen hinweg herstellen

Die NIS2-Richtlinie strebt völlig zurecht eine weitgehende Vereinheitlichung der Cybersicherheit über die Verwaltung und die anderen wichtigen Sektoren an. Es soll übergreifend ein Mindestsicherheitsniveau erreicht werden. Die Zusammenarbeit und der Informationsaustausch zwischen Organisationen soll verbessert werden, wodurch Kosten reduziert und Synergieeffekte genutzt werden können. Ein organisationsübergreifendes Vorgehen verbessert die Angriffserkennung und Lagebilderstellung und sie vereinfacht und beschleunigt die Abwehr.

Werden einzelne wichtige Einrichtungen oder ganze Sektoren herausgenommen oder die Anwendung für optional erklärt, verzichtet man umgekehrt auf ein einheitliches Mindestniveau, vergibt Synergieeffekte und akzeptiert eine Verschlechterung der Erkennung und Abwehr für alle.

---

[2] Haya Schulmann, Michael Waidner: Von Desinformation zur kognitiven Kriegsführung; FAZ 13.11.2023
https://www.faz.net/aktuell/wirtschaft/cybersicherheit-von-deep-fakes-zur-kognitiven-kriegsfuehrung-19310389.html

Leider enthält der vorliegende Gesetzesentwurf bereits auf der Bundesebene, die eigentlich komplett durch das Gesetz abgedeckt werden sollte, durch § 29 eine Vielzahl solcher Ausnahmen. Einrichtungen werden teilweise ganz ausgenommen (z.B. das Auswärtige Amt), teilweise wird die Anwendung für optional erklärt. Diese Ausnahmen sollten vermieden und auf das Notwendigste reduziert werden. Ausnahmen sollten zudem inhaltlich nachvollziehbar begründet sein.

Eine weitere, unserer Meinung nach ungerechtfertigte und kontraproduktive Ausnahme betrifft die Forschung. Forschungseinrichtungen gehören laut Anlage 1 des BSIG zu den "wichtigen Einrichtungen". Die Liste der Cyberangriffe auf Forschungseinrichtungen steigt stetig an. Unsere eigenen Studien in ATHENE zur Sicherheit der Universitäten und außeruniversitären Forschung belegen die sehr hohe Verwundbarkeit gerade dieses Sektors.[3] §2(12) stellt allerdings klar, dass mit "Forschungseinrichtungen" im NIS2-Umsetzungsgesetz nur solche gemeint sind, die primär, also zu mehr als 50%, angewandte Forschung und experimentelle Entwicklung im Hinblick auf kommerzielle Zwecke durchführen. Damit verschärft das NIS2-Umsetzungsgesetz die Sprechweise der NIS2-Richtlinie. Alle Universitäten sind damit ausgeklammert, ebenso wie die außeruniversitären Forschungsgesellschaften mit Ausnahme der Fraunhofer-Gesellschaft. Angesichts der Bedeutung der Forschung insgesamt, der vielen Cyberangriffe und der unzureichenden Cybersicherheit in diesem Sektor sollte diese Ausnahme gestrichen werden. Forschungseinrichtungen sollten generell als wichtige Einrichtungen im Sinne des NIS2-Umsetzungsgesetzes gelten. Ausnahmen sollten sich auch hier an Größe und Risiko orientieren.

Das NIS2-Umsetzungsgesetz betrifft unmittelbar nur die Verwaltungen auf Bundesebene, die Verantwortung für die Umsetzung auf Landesebene liegt bei den Ländern. Durch die Länder wiederum wurden die kommunalen Verwaltungen und die Hochschulen aus der NIS2-Umsetzung ausgenommen. Damit ist eine uneinheitliche Vorgehensweise zwischen den Ländern vorprogrammiert, und es werden zwei besonders wichtige, aber auch besonders angreifbare Sektoren komplett herausgenommen.

Aufgrund der bestehenden Verantwortungsverteilung zwischen Bund und Ländern kann das NIS2-Umsetzungsgesetz an diesem Umstand zwar nichts ändern. Dennoch stellt diese Aufteilung ein erhebliches Cyber-Sicherheitsrisiko für Deutschland dar und sollte deshalb dringend durch die Gesetzgeber in Bund und Land überdacht und geändert werden.

In den Ländern haben sich unterschiedliche IT-Architekturen entwickelt, die sich auf die Implementierungsdetails der Cybersicherheit auswirken können. Insgesamt haben aber alle Verwaltungen, Bund und Länder, mehr oder weniger dieselben

[3] Haya Schulmann, Michael Waidner: Kein Fortschritt an Hochschulen; Behörden Spiegel, November 2024, Seite 30

Cyber-Sicherheitsprobleme. Damit haben alle Verwaltungen, Bund und Land, nahezu identische Bedarfe an Wissen und Schulungen, Scans und Analysen, Mindestanforderungen, Hilfestellungen. Hinzu kommt, dass verwundbare Verwaltungen – egal auf welcher Ebene – für Cyberangreifer ein besonders attraktives Sprungbrett zum Angriff auf weitere Organisationen darstellen. Solche Sprungbretter dienen z.B. zum sehr überzeugenden Phising, zur Verteilung von Schadsoftware, zur Verbreitung und Kontrolle eines Botnetzes. Je höhe die Reputation eines solchen Sprungbretts, desto attraktiver ist es für Cyberangreifer.

Es wäre deshalb wünschenswert, wenn sich Bund, Länder und Kommunen auf ein gemeinsames Vorgehen einigen würden. Der unten vorgeschlagene Expertenrat könnte die dafür notwendigen Analysen und Empfehlungen entwickeln.

Empfehlung 2:
Nationale Cyber-Sicherheitsorganisation stärken

Deutschland verfügt auf Bundesebene mit dem BSI über eine etablierte und gut funktionierende zentrale Cyber-Sicherheitsbehörde und damit im Kern über eine gute nationale Cyber-Sicherheitsarchitektur.

Mit §48 wird die Position eines Koordinators für Informationssicherheit auf Bundesebene eingeführt, also ein “CISO Bund”, allerdings ohne diese Position inhaltlich oder strukturell näher zu beschreiben. In der Fachwelt herrscht weitgehend Einigkeit, was die Rechte und Pflichten eines CISO bzw. einer CISO-Organisation sind. Besonders wichtig sind eine hohe persönliche Fachkompetenz, die strategische und operative Verantwortung für die Cybersicherheit der Organisation, die Möglichkeit der direkten Berichterstattung an die obersten Entscheidungsträgern und ein qualifiziertes Vetorecht gegenüber allen Maßnahmen innerhalb der Organisation (also hier des Bundes), die sich negativ auf die Cybersicherheit auswirken könnten. Ein CISO ist stets Teil der Organisation, für deren Cybersicherheit er verantwortlich ist, benötigt aber ein hohes Maß an Autonomie hinsichtlich Kommunikation in und außerhalb der Organisation und hinsichtlich der Ausübung seines Vetorechts.

Die Funktion des CISO Bund sollte in §48 entsprechend konkretisiert werden. Die meisten der üblichen CISO-Funktionen liegen heute und auch nach dem NIS2-Umsetzungsgesetz beim BSI. Die CISO-Funktion sollte daher dem BSI zugeordnet werden. Andernfalls besteht die Gefahr kontraproduktiver Doppelstrukturen und einer Gefährdung der Autorität und Autonomie des BSI.

Es ist zu begrüßen, dass das NIS2-Umsetzungsgesetz die Rolle und Stellung des BSI als Bundesoberbehörde im Geschäftsbereich des BMI grundsätzlich unverändert lässt. Ein

CISO sollte generell unabhängig vom CIO sein, und entsprechend sollte die Autonomie des BSI gegenüber dem BMI gestärkt werden, etwa indem die Fachaufsicht durch das BMI auf das Notwendigste beschränkt wird und das BSI volle Autonomie hinsichtlich der Kommunikation mit anderen Behörden und nach außen erhält. Eine vollständige Unabhängigkeit ist für die meisten Aufgaben des BSI aber weder notwendig noch hilfreich.

Wie oben erläutert, ist es für die Cybersicherheit in Deutschland wichtig, die derzeitige föderale Cyber-Sicherheitsarchitektur zu einer einheitlichen, nationalen Cyber-Sicherheitsarchitektur umzubauen und das BSI zu einer Zentralstelle für Cybersicherheit auch für die Länder und Kommunen zu entwickeln. Das NIS2-Umsetzungsgesetz kann aufgrund der derzeitigen Kompetenzverteilungen zwischen Bund und Ländern eine so weitreichende Änderung zwar nicht leisten, aber ich halte dies für eine der wichtigsten strategischen Empfehlungen für Bundestag und die Landesparlamente zur Verbesserung der Cybersicherheit in Deutschland.

Die wissenschaftlich-technische Fachwelt steht nahezu einhellig hinter dieser Empfehlung, dennoch scheitert bislang die politische Umsetzung. Um in Zukunft solche und ähnlich wichtige und grundsätzliche Entscheidungen fachlich und unabhängig von anderen politischen Erwägungen vorbereiten zu können, empfehlen wir die Einrichtung eines unabhängigen Expertenrates für Cybersicherheit der Bundesregierung. Dieser Rat sollte aus unabhängigen Sachverständigen aus Forschung, Gesellschaft, Wirtschaft und Verwaltung mit großer, ausgewiesener persönlicher Fachexpertise bestehen. Die Berufung von Funktionsträgern ohne ausgewiesene persönliche Expertise in der Cybersicherheit muss vermieden werden. Der Rat sollte regelmäßig die Cybersicherheitslage in Deutschland begutachten und auch quantitativ anhand von beauftragten und eigenen Studien bewerten. Er sollte eine inhaltlich treibende Rolle bei der Weiterentwicklung und Umsetzung der Cybersicherheitsstrategie Deutschlands übernehmen und hierzu mit hoher Kompetenz entsprechende Empfehlungen aussprechen können.

Empfehlung 3:
Erweiterte Lagebilderstellung

Für die Cybersicherheit einer Organisation, eines Sektors, eines Landes ist es entscheidend, jederzeit über ein möglichst aktuelles, umfassendes und qualitativ hochwertiges Bild der eigenen IT und ihrer Verwundbarkeiten, der Anzeichen für laufende oder frühere erfolgreiche Angriffe (z.B. im Darknet), derzeit eingesetzte Angriffstechniken und aktive Angreifer, und weiterer Risikofaktoren zu haben. Solche Lagebilder unterstützen die Abwehr aktueller Angriffe, die Priorisierung von Maßnahmen und die Bewertung der Entwicklung von Risiken und der Cybersicherheit

insgesamt über die Zeit. Die Erstellung von Lagebildern ist technisch anspruchsvoll; die Fortentwicklung ist eines der zentralen Themen der angewandten Forschung und Entwicklung in ATHENE. Vollständigkeit, Qualität und Aufwand der Lagebilderstellung profitieren sehr deutlich davon, Lagebilder über größere, zusammenhängende Einheiten hinweg zu erstellen.

Es ist zu begrüßen, dass das NIS2-Umsetzungsgesetzes insbesondere in § 15 dem BSI eine zentrale Rolle in der Lagebilderstellung gibt. Wie schon an anderer Stelle erwähnt, wäre es vorteilhaft, diese Lagebilderstellung nicht nur auf die Bundesverwaltung und (besonders) wichtige Einrichtungen zu beschränken, sondern zumindest auch die Länder und als Angebot weitere Einheiten von Wirtschaft und Gesellschaft einzubeziehen. Je umfassender das Lagebild ist, desto wertvoller ist es für die Verbesserung der nationalen Cybersicherheit.

Entscheidend ist, in die Lagebilderstellung nicht nur die IT der Einrichtungen selbst einzubeziehen, sondern auch die IT der jeweiligen Lieferketten, also z.B. externe Dienstleister, Cloud-Computing-Dienstleister. Nur so kann ein Gesamtbild entstehen. Dies bedeutet, dass das BSI beispielsweise auch die IT-Infrastrukturen (Netzes, Server) von Cloud-Computing-Diensten und anderer externer Dienstleister scannen muss, auch wenn diese sich im Ausland und außerhalb der Aufsichtspflicht des BSI befinden.

Darüber hinaus sollte ergänzt werden, dass die Formulierung in §15(1) nicht bedeutet, dass das BSI nur bekannte Schwachstellen identifizieren darf. Die Erläuterung zum Gesetzesentwurf, “§ 15 ermächtigt indes nicht zur Entdeckung von besonders sensiblen, unbekannten Schwachstellen (auch: Zero-Day-Schwachstellen).” legt allerdings nahe, dass genau dies gemeint ist. Tatsächlich sollte das BSI ausdrücklich auch Zero-Day-Schwachstellen aufdecken dürfen, da diese eine besonders große Gefahr darstellen. Bedenken, dass Zero-Day-Schwachstellen vom BSI zurückgehalten und an andere Behörden weitergegeben werden könnten, könnten leicht durch eine entsprechend konkretisierte Verpflichtung zur zeitnahen Information an die Hersteller ausgeräumt werden.

In § 59 wird das BSI als zuständige Aufsichtsbehörde für alle (besonders) wichtigen Einrichtungen, kritischen Anlagen und Einrichtungen der Bundesverwaltung benannt. In § 60 wird dies für internationale Einrichtungen auf diejenigen eingeschränkt, die ihren Hauptsitz in Deutschland haben. Dies ist sinnvoll, um Doppelungen in den Zuständigkeiten zu vermeiden, bedeutet aber, dass ein Großteil der Lieferketten nicht der Aufsicht des BSI unterstellt ist. Es muss sichergestellt sein, dass in der praktischen Umsetzung das BSI auch diese Teile der Lieferketten vollumfänglich in die eigene Lagebilderstellung einbeziehen und z.B. scannen und analysieren kann, und dies auch tatsächlich tut.

Empfehlung 4:
Konkrete Verpflichtungen jenseits IT-Grundschutz

In § 4(2) wird für das Bundeskanzleramt und die Bundesministerien die Umsetzung des IT-Grundschutzes verbindlich vorgeschrieben. Dies ist sehr zu begrüßen und sollte auf alle betrachteten Einrichtungen ausgeweitet werden.

Generell sind konkrete Vorgaben sehr zu begrüßen. Der IT-Grundschutz deckt allerdings nicht alle notwendigen Bereiche der Cybersicherheit ab. Sinnvoll wäre beispielsweise ebenso die verbindliche Umsetzung von Zero-Trust-Prinzipien, ähnlich wie dies im Mai 2021 durch die Bundesregierung der USA per Executive Order für die US-Bundesverwaltung gemacht wurde.[4]

Völlig zurecht spielt in der NIS2-Richtlinie die Sicherheit des Internets eine herausragende Rolle. Das Internet ist die mit Abstand größte und wichtigste und damit auch kritischste Kommunikationsinfrastruktur unserer Zeit. In § 28 (2) werden als besonders wichtige Einrichtungen unter anderen Top Level Domain Name Registries und DNS-Diensteanbieter genannt. Dies ist zu begrüßen, blendet aber aus, dass es neben DNS weitere, für die Internetsicherheit genauso wichtige Systeme gibt. Zu nennen ist hier insbesondere die Routing-Sicherheit, für die RPKI das zentrale System ist. Auch hier hat die US-Bundesregierung ein gutes Beispiel gegeben mit der im September 2024 vom White House veröffentlichten "Roadmap to enhancing Internet Routing Security", die verbindliche Vorgaben für die Netzbetreiber der USA macht.[5] Diese Roadmap bezieht sich ausführlich auf unsere Forschung und die Empfehlungen, die wir in ATHENE gemacht haben.

Empfehlung 5:
Aktive Maßnahmen zur Cyberabwehr

Das NIS2-Umsetzungsgesetz bewahrt die bestehenden, sehr begrenzten Möglichkeiten des BSI, aktiv gegen laufende und absehbare Cyberangriffe vorzugehen, erweitert aber in keiner Weise die Möglichkeiten des BSI oder anderer Behörden für weitere aktive Maßnahmen zur Cyberabwehr wie z.B. in unserem Artikel in der FAZ vom 25. April 2022 beschrieben.[6] Es wäre wünschenswert, als Teil der nationalen

---

[4] https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

[5] Report by the White House Office of the National Cyber Director: Roadmap to Enhancing Internet Routing Security; Washington DC, September 2024
https://www.whitehouse.gov/wp-content/uploads/2024/09/Roadmap-to-Enhancing-Internet-Routing-Security.pdf

[6] Haya Schulmann, Michael Waidner: Der Weg zur aktiven Cyberabwehr, FAZ 25.04.2022
https://www.faz.net/pro/digitalwirtschaft/cybersicherheit-der-weg-zur-aktiven-cyberabwehr-17980091.html; leicht überarbeitet
https://www.forschung-it-sicherheit-kommunikationssysteme.de/dateien/forschung/2023-03-impulspapier-aktive-cyberabwehr.pdf

Cyber-Sicherheitsarchitektur einen vollständigen Rechtsrahmen auch für diese Maßnahmen zu schaffen.

Empfehlung 6:
Vertrauenswürdige IT

Eine der zentralen und bislang nicht zufriedenstellend gelösten Herausforderungen für die Cybersicherheit ist die Sicherstellung eines ausreichenden Angebots an geeigneten und vertrauenswürdigen IT-Lösungen, insbesondere im Bereich der Cybersicherheit. Die große und asymmetrische Abhängigkeit Deutschlands in der Digitalisierung, IT und IT-Sicherheit wie auch die Auswirkung auf unsere digitale Souveränität sind hinlänglich bekannt.[7]

Einerseits braucht es mehr und international erfolgreiche innovative Unternehmen in Deutschland und Europa, die aufgebaut und gefördert werden müssen, andererseits müssen wir Methoden entwickeln und anwenden, wie Angebote als nicht vertrauenswürdig erkannt und vom Markt teilweise oder ganz ausgeschlossen werden können.

Diese Aspekte werden im NIS2-Umsetzungsgesetz kaum bzw. nur indirekt behandelt. Es gibt einen großen Fokus auf Zertifizierungen. Diese funktionieren aber letztlich nur dann gut, wenn ein Produkt oder Dienst von einem a priori vertrauenswürdigen Hersteller oder Dienstleister kommt.

Die Möglichkeiten des BSI, Warnungen aufgrund erkannt mangelhafter Vertrauenswürdigkeit auszusprechen, werden durch das NIS2-Umsetzungsgesetz weder konkretisiert noch geändert. Wie problematisch dies ist, zeigte sich 2022 in der Diskussion um die Warnung des BSI vor der Antivirensoftware des russischen Herstellers Kaspersky.[8] Diese Warnung war unserer Meinung nach notwendig und berechtigt, ihre Rechtmäßigkeit wurde aber von vielen in Zweifel gezogen. Die Möglichkeiten, vor Produkten aber auch vor einzelnen Herstellern zu warnen, sollten deutlich konkretisiert und ausgeweitet werden.

---

[7] Haya Schulmann, Michael Waidner: Wieso Deutschland in digitaler Abhängigkeit verharrt, FAZ 27.06.2024
https://www.faz.net/aktuell/wirtschaft/unternehmen/digitale-souveraenitaet-warum-deutschland-in-abhaengigkeit-verharrt-19809000.html

[8] Haya Schulmann, Michael Waidner: Wie Deutschland mit nicht vertrauenswürdiger IT besser umgehen kann; FAZ 24.10.2022
https://www.faz.net/pro/digitalwirtschaft/kaspersky-virenschutz-wie-deutschland-it-systeme-besser-schuetzen-kann-18408167.html

Deutscher Bundestag

Ausschuss für Inneres und Heimat

Ausschussdrucksache
20(4)523 I

bitkom

Stellungnahme

November 2024

NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz

Zusammenfassung

Angesichts der Cyberbedrohungslage unterstützt der Bitkom die Harmonisierung des Cybersicherheitsniveaus durch das NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG). Im Regierungsentwurf bewerten wir den konsequenten Austausch der Begrifflichkeit von „Cybersicherheit“ zu „Informationssicherheit“ als positiv. So werden durch einen holistischen Ansatz alle technischen und organisatorischen Aspekte zum Schutz von Informationen, sowohl analog als auch digital, einbezogen. Die geplante Online-Plattform zum Informationsaustausch zwischen wichtigen Einrichtungen und der Bundesverwaltung ist ein guter Schritt. Das BSI sollte die Entwicklung unbedingt in Abstimmung mit der Wirtschaft voranbringen.

Auf der anderen Seite wurde der Großteil der von der Wirtschaft aufgezeigten Änderungsbedarfe im Regierungsentwurf nicht aufgenommen. Dadurch bestehen weiterhin Rechtsunsicherheiten für die Wirtschaft. Insbesondere KMU können ihre Betroffenheit vom NIS2UmsuCG oft nicht selbst abschätzen. Für mehr Rechtssicherheit muss der Referentenentwurf mit dem KRITIS-Dachgesetz abgestimmt werden. Eine fehlende Konsultation führt ansonsten zu Auslegungsproblemen und Konflikten zwischen Behörden. Für Dienste nach § 30, die in verschiedenen Geschäftsbereichen erbracht werden, empfehlen wir, die Definition auf die für kritische Dienstleistungen verwendeten IT-Systeme zu beschränken oder zumindest klarzustellen, dass unterschiedliche Risiken in die Risikobewertung einbezogen werden sollten.

Darüber hinaus kritisieren wir die Ausnahme von Einrichtungen der Bundesverwaltung und kommunaler Verwaltungen von den NIS2UmsuCG-Vorgaben. Behördliche und kommunale Dienstleistungen sind zentral für das tägliche Leben in Deutschland. Ein grundlegender Sicherheitsrahmen muss daher eingeführt werden, um diese Bereiche zu schützen. Die Hauptlast der Maßnahmen wird allein auf die Privatwirtschaft abgewälzt. Während diese Ihre volle Verantwortung annimmt, sehen wir mit Sorge, dass dies von staatlicher Seite nicht erfolgt. Somit bleiben Verwaltung und staatlich Einrichtungen die Schwachstelle für die Cybersicherheit in Deutschland. Eine integrative Herangehensweise, die alle Verwaltungsebenen einbezieht, ist notwendig, um die Cybersicherheit in der Breite zu erhöhen. Der Bitkom appelliert daher an die Bundesregierung, sich auch bei den Ländern und Kommunen für einen inklusiven Ansatz einzusetzen.

97%

der deutschen Unternehmen finden, dass Sicherheitsbehörden sie besser über die Cybersicherheitslage informieren sollten. (Bitkom, 2023)

Allgemeine Anmerkungen

Die Bedrohungslage im Cyberraum bleibt angespannt. Im vergangenen Jahr ist der deutschen Wirtschaft allein durch Cyberattacken ein Schaden in Höhe von 148,2 Mrd. Euro entstanden und die Unternehmen gehen davon aus, dass dies weiter stark ansteigen wird (Bitkom, 2023). Vor diesem Hintergrund ist es unerlässlich, die gesetzliche Verankerung und Governance der Informationssicherheit in Deutschland weiterzuentwickeln. Mit der NIS-2-Richtlinie (EU) 2022/2555 wurde auf europäischer Ebene dafür ein guter Kompromiss mit einer vernünftigen Balance zwischen gezielten regulatorischen Eingriffen und einer ganzheitlichen Stärkung der Cyber-Resilienz der EU gefunden.

Der Bitkom ist weiterhin überzeugt von der europäischen Idee für einen ganzheitlich gestärkten und harmonisierten Cybersecurity-Regulierungsrahmen. Wir begrüßen die Ziele des NIS2UmsuCG und die Möglichkeit zur Beteiligung an der öffentlichen Anhörung. Es ist positiv zu bewerten, dass das Gesetz den Betreibern Kritischer Anlagen eine Frist von mindestens drei Jahren gewährt, um die Erfüllung der Anforderungen nach § 30 Abs. 1 erstmals dem BSI gegenüber nachzuweisen. Ebenso begrüßen wir die ersatzlose Streichung der Kategorie „Unternehmen im besonderen öffentlichen Interesse“, wodurch künftig neben Kritischen Anlagen nur noch wichtige sowie besonders wichtige Einrichtungen berücksichtigt werden. Dies trägt zur Stärkung der europaweiten Harmonisierung der Cybersicherheitsregulierung bei und beendet den deutschen Sonderweg des IT-Sicherheitsgesetzes 2.0.

Durch die verpasste Umsetzungsfrist im Oktober 2024 entstehen zweierlei Probleme. Erstens schadet dies der EU-weiten Harmonisierung in der Cybersicherheit, da andere Mitgliedsstaaten bereits fortgeschritten sind und damit andere Umsetzungsfristen gelten. Zweitens entsteht durch die Verzögerung eine Rechtsunsicherheit für Unternehmen. Viele Unternehmen, insbesondere KMU, können nicht ohne externe Beratung ihre Betroffenheit vom NIS2UmsuCG absehen oder sind sich gar nicht bewusst, dass sie möglicherweise in den Geltungsbereich fallen. Auch bei größeren, europaweit agierenden Unternehmen besteht Verunsicherung hinsichtlich verschiedener Umsetzungen in verschiedenen Mitgliedsstaaten. Wir bitten in Hinblick auf diese genannten Punkte um Klarstellung seitens des Gesetzgebers.

Bei der Weiterentwicklung der Cybersicherheitsstrategie Deutschlands ist auch zu beachten, dass diese eng mit der Nationalen Sicherheitsstrategie und dem KRITIS-Dachgesetz abgestimmt sein muss, um ein kohärentes und konsistentes Vorgehen zu gewährleisten. Die NIS-2-Richtlinie (EU) 2022/2555 sieht in Artikel 7 lit. g „eine verstärkte Koordinierung zwischen den [...] zuständigen Behörden [...] zum Zweck des Informationsaustauschs über Risiken, Bedrohungen und Sicherheitsvorfälle“ vor. Es gilt daher mit dem NIS2UmsuCG und dem KRITIS DachG ein einheitliches Verständnis darüber zu entwickeln, wie physische Sicherheit und Cybersicherheit gemeinsam umgesetzt werden können. In der Unternehmenspraxis sind diese Bereiche eng miteinander verzahnt und sollten nicht isoliert voneinander betrachtet und umgesetzt werden müssen. Aktuell führt fehlende Konsultation der Gesetzentwürfe zu uneinheitlichen Definitionen und Begrifflichkeiten, die Auslegungsprobleme verursachen können. Dies zeigt sich beispielsweise in den konfliktbehafteten Zuständigkeiten vom BSI im NIS2UmsuCG auf der einen Seite und dem BBK im KRITIS

DachG auf der anderen Seite. Die angestrebte EU-weite Harmonisierung der Cybersicherheit kann auf dieser Grundlage nicht ausreichend erreicht werden. NIS2UmsuCG und das KRITIS DachG sollten daher stärker aufeinander abgestimmt und wesentliche Regelungsinhalte im Sinne des All-Gefahren-Ansatzes besser harmonisiert werden. Die zügige Novellierung der BSI-KRITIS-Verordnung ist ebenfalls von Bedeutung, um Sektoren anhand von Schwellwerten und Anlagekategorien zu definieren.

Die Entscheidung, kommunale Verwaltungen auf Wunsch der Länder sowie Bundeseinrichtungen von den Vorgaben des NIS2UmsuCG auszunehmen, wird in unserer Mitgliedschaft mit Sorge aufgenommen. Kommunale Dienstleistungen sind von zentraler Bedeutung für das tägliche Leben der Bürgerinnen, Bürger und Unternehmen. Ein Ausfall essenzieller Dienste würde nicht nur unmittelbare und erhebliche Auswirkungen auf die betroffene Bevölkerung und Wirtschaft haben, sondern könnte auch das Vertrauen in die Funktionsfähigkeit staatlicher Strukturen nachhaltig erschüttern. Vor diesem Hintergrund ist eine Stärkung der Cybersicherheit in diesen Bereichen unabdingbar und von höchster Priorität. Auch wenn der Bund hier nur eingeschränkten Einfluss hat, fordern wir dennoch einen verstärkten Einsatz für die Harmonisierung von Cybersicherheitsstandards auf allen Ebenen in Deutschland. Anstatt aus Gründen des vermeintlich hohen Aufwands auf spezifische Vorgaben für die Kommunen zu verzichten, wäre die Einführung eines grundlegenden Sicherheitsrahmens, eine angemessene und praktikable Alternative. Ein solcher Rahmen könnte beispielsweise bei Asylverfahren den notwendigen Schutz für eingestufte Daten gewährleisten, ohne die Ressourcen der kommunalen Verwaltungen übermäßig zu belasten. Dafür stehen bereits heute eine Vielzahl an etablierten Standards zur Absicherung zu Verfügung, die den Kommunen auch im „Weg in die Basis-Absicherung“ (WiBA) an die Hand gegeben werden.

Es ist aus unserer Sicht nicht nachvollziehbar, dass die Hauptlast der Umsetzung der Cybersicherheitsmaßnahmen erneut auf die Privatwirtschaft abgewälzt wird, während wesentliche Teile der öffentlichen Verwaltung ausgenommen bleiben. Dies steht in direktem Widerspruch zum erklärten Ziel der NIS-2-Richtlinie (EU) 2022/2555, die Resilienz und Sicherheit in der Daseinsvorsorge umfassend zu stärken. Eine integrative Herangehensweise, die auch die kommunalen Verwaltungen einschließt, ist unerlässlich, um die Cybersicherheit in allen Bereichen des öffentlichen Lebens zu erhöhen. Wir appellieren daher an das BMI, die bestehenden Ausnahmen zu überdenken und in Zusammenarbeit mit den Ländern einen inklusiven Ansatz zu verfolgen, der den Schutz und die Sicherheit der gesamten Bevölkerung gewährleistet.

Um Unternehmen und Behörden noch effektiver zu schützen, schlagen wir zudem vor, dass neben organisatorischen und technischen Maßnahmen auch die Mitarbeitenden in die Sicherheitsstrategien einbezogen werden. Regelmäßige Schulungen und Sensibilisierungsprogramme sind hierbei entscheidend. Die Überprüfung der Vertrauenswürdigkeit von Mitarbeitenden in sicherheitsrelevanten Bereichen kann zur Unternehmensresilienz beitragen. Derzeit fehlt jedoch eine gesetzliche Grundlage, die eine rechtssichere Prüfung von Bewerbenden, Mitarbeitenden und Dienstleistenden ermöglicht. Eine möglicher Lösungsansatz wäre die Option zur freiwilligen Vertrauenswürdigkeitsüberprüfung aus Artikel 14 der Resilience-of-Critical-Entities-Richtlinie ((EU) 2022/2557) in die deutschen Gesetze zu übernehmen. Diese Prüfung

sollte durch staatliche Stellen erfolgen, wofür ein geeigneter rechtlicher Rahmen dafür zu schaffen ist. Die Überprüfung soll zudem die bestehende staatliche Sicherheitsüberprüfung im Geheim- und vorbeugenden personellen Sabotageschutz ergänzen und nahtlos in das bestehende System integriert werden.

Wir möchten an dieser Stelle außerdem darauf hinweisen, dass die wörtliche Übersetzung des Begriffs „Access Control“ zu einer fehlerhaften Interpretation führen kann. Statt dem bisher gewählten Wort „Zugriffskontrolle“ scheint vielmehr „Zugriffssteuerung“ die Bedeutung im Sinne der europäischen Richtlinie wiederzugeben.

Artikel 1: Gesetz über das Bundesamt für Sicherheit in der Informations-technik und über die Sicherheit in der Informationstechnik von Einrichtungen

§ 2 Begriffsbestimmungen

Um eine einheitliche Gestaltung der Meldepflichten in allen EU-Mitgliedsstaaten sicherzustellen, sowohl hinsichtlich der zu meldenden Vorfälle als auch ihrer Auswirkungen, ist es von entscheidender Bedeutung, dass die Mitgliedsstaaten eine gemeinsame Auslegungspraxis vereinbaren. Statt nationale Begriffsbestimmungen zu entwickeln, sollte die Bundesregierung im Rahmen der Umsetzung von Artikel 23 der NIS-2-Richtlinie (EU) 2022/2555 gemeinsam mit anderen Mitgliedsstaaten dieses gemeinsame Verständnis erarbeiten. Dies würde dazu beitragen, eine kohärente und einheitliche Umsetzung der Meldepflichten zu gewährleisten.

Die „Kommunikationstechnik des Bundes“, die in § 2 Abs. 21 als Informationstechnik, die von einer oder mehreren Einrichtungen der Bundesverwaltung oder im Auftrag einer oder mehrerer Einrichtungen der Bundesverwaltung betrieben wird beschrieben wird, ist aus unserer Sicht zu wenig abgrenzungsscharf und sollte klarer definiert werden.

Aktuell besteht aus unserer Sicht die Gefahr einer Überregulierung für Rechenzentrumsbetreiber, da gemäß § 2 Abs. 1 Nr. 35 eine weitreichende Einbeziehung aller benötigten Anlagen und Infrastrukturen, insbesondere der für die Stromverteilung, vorgesehen ist. Diese Regulierung geht über die Anforderungen der EU hinaus und könnte zu unnötigen Belastungen führen. Es ist daher wichtig, eine angemessene Balance zwischen Sicherheitsanforderungen und wirtschaftlicher Tragfähigkeit zu wahren, um die Effizienz und Wettbewerbsfähigkeit der betroffenen Unternehmen nicht zu gefährden.

§ 3 Aufgaben des Bundesamtes

In Artikel 24 Absatz 1 Satz 2 der NIS-2-Richtlinie (EU) 2022/2555 heißt es: „Darüber hinaus fördern die Mitgliedstaaten, dass wesentliche und wichtige Einrichtungen

qualifizierte Vertrauensdienste nutzen.“ Dieser Aspekt findet jedoch im aktuellen Referentenentwurf für ein NIS2UmsuCG keine Berücksichtigung. Wir regen an, diesen Verweis im NIS2UmsuCG aufzunehmen, um durch das Gesetz sicherzustellen, dass Maßnahmen zur breiten Implementierung qualifizierter Vertrauensdienste gefördert werden. Generell befürworten wir auch andere Maßnahmen, die diese Zielsetzung unterstützen.

§ 6 Informationsaustausch

Wir begrüßen, dass das BSI eine Online-Plattform zum Informationsaustausch mit wichtigen Einrichtungen und der Bundesverwaltung betreiben wird. Es ist essenziell, dass BMI und BSI vorab eine Testversion des BSI Information Sharing Portals vorlegen und es gemeinsam mit der Wirtschaft weiterentwickeln, um zielgruppengerechte Lageinformationen bereitzustellen. Wir stehen bereit, um uns am Austausch dazu zu beteiligen und konstruktives Feedback zu geben.

Für die Vorgabe der Teilnahmebedingungen auf der Online-Plattform nach § 6 Abs. 2 durch das BSI sollten hohe operative Aufwände vermieden werden, um auch KMU eine niedrigschwellige Beteiligung am Informationsaustausch zu ermöglichen. Auch eine Vereinheitlichung der Plattform zur Umsetzung von Informationspflichten aus anderen Gesetzesvorhaben wie dem KRITIS DachG würde weiter zu einer lösungsorientierten Nutzung beitragen. Neben dem digitalen Austausch von Informationen ist es wichtig, den Umsetzungsplan KRITIS (UP KRITIS) fortzusetzen, um den persönlichen und vertrauensvollen Kontakt zwischen den Beteiligten zu gewährleisten.

§ 14 Untersuchung der Sicherheit in der Informationstechnik, Auskunftsverlangen

Das BSI kann zur Erfüllung seiner Aufgaben informationstechnische Produkte und Systeme untersuchen und ist berechtigt, von den Herstellern alle erforderlichen Auskünfte, insbesondere über technische Einzelheiten, zu verlangen. Die aus den Untersuchungen gewonnenen Erkenntnisse dürfen weitergegeben und veröffentlicht werden, wenn dies der Aufgabenerfüllung dient. Bis zum Inkrafttreten des CRA als EU-weit geltender Rechtsrahmen für Produkte mit digitalen Elementen, ist das hier vorgesehene Vorgehen eine angemessene Übergangslösung. Ab dem Inkrafttreten des CRA muss unbedingt gewährleistet werden, dass es keine parallelen Formen der Marktaufsicht gibt.

Aktuell geht jedoch weder aus dem Gesetzentwurf noch aus der Begründung hervor, wie sichergestellt werden soll, dass einerseits das Interesse der Allgemeinheit an der Aufklärung von Sachverhalten und andererseits das Interesse des Herstellers an der Geheimhaltung produkt- oder servicebezogener Informationen gewahrt bleibt. Insbesondere ist das Verhältnis der entsprechenden Auskunftsrechte zum GeschGehG gänzlich unklar. Der Gesetzgeber muss daher sicherstellen, dass das BSI ein Verfahren etabliert, welches, soweit technisch und prozedural möglich, den Schutz von Betriebs- und Geschäftsgeheimnissen gewährleistet und die Gefahr von Industriespionage minimiert.

Wenn für eine Schwachstelle kein schneller Patch verfügbar ist, sollte diese nur intern kommuniziert werden. Dies verhindert, dass Kunden und Betreiber durch die Veröffentlichung von Angriffsmöglichkeiten geschädigt werden. Das BSI muss die Hersteller über die Beschreibung der Angriffsmöglichkeit sowie rechtzeitig vor der Veröffentlichung über den Inhalt der vom BSI geplanten externen Kommunikation informieren. Den Herstellern ist, im Sinne des Responsible Disclosure Verfahrens, vor der Veröffentlichung ausreichend Zeit zur Behebung des Problems einzuräumen.

§ 28 Besonders wichtige Einrichtungen und wichtige Einrichtungen

Während privatwirtschaftliche Unternehmen die Anforderungen erfüllen müssen, bleiben relevante kommunale Einrichtungen weiterhin vom Anwendungsbereich ausgeschlossen, mit Verweis auf die konkurrierende Gesetzgebung der Länder. Dies ist für eine ganzheitliche nationale Cybersicherheitsabwehr weder förderlich noch akzeptabel. Lediglich wenn diese Einrichtungen Waren oder Dienstleistungen gegen Entgelt für Einrichtungen der Bundesverwaltung anbieten, fallen sie in den Anwendungsbereich des Gesetzes (Artikel 1 § 28 Abs. 9). Dadurch wird versäumt, eine einheitliche Cybersicherheitsstrategie zu entwickeln, die ein hohes Niveau der Cybersicherheit auf allen Ebenen der Verwaltung ermöglicht. Wir sprechen uns daher dafür aus, in Koordination mit den Ländern auch kommunale Einrichtungen in den Anwendungsbereich des NIS2UmsuCG aufzunehmen.

Des Weiteren bleibt problematisch, dass neben der Einordnung in wichtige und besonders wichtige Einrichtungen zusätzlich der Begriff "Betreiber kritischer Anlagen" verwendet wird. Die Identifikation, welche Einrichtungen nun tatsächlich im Geltungsbereich der Anforderungen des novellierten BSIG unterliegen, kann sich unter Umständen als sehr aufwändig gestalten. Hier wären klarstellende Kriterien im Sinne einer Checkliste äußerst hilfreich.

§ 29 Einrichtungen der Bundesverwaltung

Die anhaltenden Cyberangriffe auf Kommunen und Behörden, die teilweise weitreichende Folgen für Wirtschaft und Gesellschaft haben, verdeutlichen die Dringlichkeit, die öffentliche Verwaltung auf allen Ebenen des föderalen Staates in den Anwendungsbereich des NIS2UmsuCG einzubeziehen. Die Fälle aus Anhalt-Bitterfeld und Schwerin zeigen die Folgen, wenn wichtige Verwaltungsdienstleistungen nicht zur Verfügung stehen und dabei beispielsweise wichtige Planungs- und Genehmigungsverfahren ausgesetzt sind. Während die Verantwortung durch den weitreichenden Anwendungsbereich auch viele mittlere und kleine Unternehmen trifft, nimmt sich der Staat hier eine Sonderrolle und entzieht sich der eigentlichen Verantwortung.

Es ist unerlässlich, dass Bundesbehörden, Landes- und Kommunalbehörden einheitlich als besonders wichtige Stellen definiert werden, um sie in den Anwendungsbereich des NIS2UmsuCG einzubeziehen. Ausnahmen davon oder Einstufungen als lediglich wichtige Einrichtungen, sollten aus unserer Sicht nicht vorgenommen werden. Dafür sollte sich das BMI insbesondere in Koordination mit den Ländern einsetzen. Die

ganzheitliche Einbeziehung ist von entscheidender Bedeutung, um das beabsichtigte Ziel der NIS-2-Richtlinie (EU) 2022/2555 zu erreichen, nämlich eine EU-weite Harmonisierung der Cybersicherheit zu gewährleisten. Nur durch eine umfassende Integration aller Verwaltungsebenen kann die Wirksamkeit von Maßnahmen zur Stärkung der Cybersicherheit in der öffentlichen Verwaltung in ganz Europa gewährleistet werden.

§ 30 Risikomanagementmaßnahmen besonders wichtiger Einrichtungen und wichtiger Einrichtungen

Das Sicherheitsziel “Authentizität” wurde nach § 30 Abs. 1 nun auch in § 2 Nr. 23 gestrichen, da davon ausgegangen wird, dass dieses bereits im Ziel „Integrität“ enthalten ist. Wir möchten darauf aufmerksam machen und empfehlen dringend eine Wiederaufnahme. Authentizität wird schließlich klar in der europäischen NIS2-Richtlichinie als Sicherheitsziel benannt. Authentizität adressiert die Identitäten, insbesondere maschinelle Identitäten, die für die digitale Transformation eminent wichtig sind. Die EU-Fachgremien haben mit Absicht Authentizität als Ziel aufgenommen, da Integrität das Identitäts-Thema nicht abbildet.

Weiterer Handlungsbedarf in § 30 besteht in den unzureichenden Formulierungen im Gesetzestext bzw. in den Erläuterungen zum Verständnis des Begriffs "Erbringung ihrer Dienste", wodurch die konkrete Reichweite der Pflichten nach § 30 Abs. 1 weiterhin unklar bleibt. Ausweislich der Begründung soll der Begriff Erbringung ihrer Dienste weit verstanden werden und sich auf "sämtliche Aktivitäten der Einrichtung (beziehen), für die IT-Systeme eingesetzt werden, dies beinhaltet beispielsweise auch Büro-IT oder andere IT-Systeme, die durch die Einrichtung betrieben werden". Die NIS-2-Richtlinie (EU) 2022/2555 selbst enthält aber keine vergleichbare Konkretisierung bzw. Aussage. Unterstellt man ein derart weites Begriffsverständnis bei § 30 Abs. 1, führt das dazu, dass Unternehmen, die in verschiedenen Geschäftsbereichen tätig sind, dabei aber nur teilweise Dienste erbringen, die unter die in Anlage 1 und Anlage 2 genannten Kategorien zu fassen sind (sektorbezogene Teilbereiche), wohl ihre gesamte IT-Landschaft an den Vorgaben des § 30 Abs. 1 ausrichten müssten. Auch in großen Konzernstrukturen, die sowohl wichtige als auch besonders wichtige Anlagen umfassen, besteht Unklarheit darüber, inwieweit die jeweiligen Verpflichtungen der Bereiche voneinander abgegrenzt werden können.

Aber selbst ohne das Betreiben verschiedener Geschäftsbereiche ist unklar, warum ein derart weiter Begriff und damit die Ausdehnung der Pflichten auf die gesamte Unternehmens-IT erforderlich sind. Selbst wenn man sich vom bisherigen, bei KRITIS-Betreibern angewandten anlagenbezogenen Begriff lösen würde, ist nicht ersichtlich, warum diese Ausweitung im Hinblick auf die Schutzziele notwendig ist. Dies gilt insbesondere für die Einrichtungen, die nur aufgrund des Betriebs einer kritischen Anlage als besonders wichtige Einrichtung gelten. Ziel ist der Schutz der Versorgungssicherheit von Deutschland in bestimmten Sektoren. Sofern ein Unternehmen im verarbeitenden Gewerbe in den Anwendungsbereich fällt, sollten etwa Produktion und Logistik geschützt werden, etwa auch ein

Warenwirtschaftssystem. Aber eine allgemeine Webseite des Unternehmens muss beispielsweise keinen erheblichen Einfluss auf die Versorgungssicherheit ausüben.

Dieses Ergebnis überrascht umso mehr, da bei der Berechnung der Schwellenwerte zur Ermittlung des Anwendungsbereichs nach § 28 nur die Kennzahlen berücksichtigt werden sollen, die auf den sektorbezogenen Teilbereich des Unternehmens entfallen (Begründung zu § 28 Abs. 3, S. 144). Damit soll sichergestellt werden, dass Unternehmen, "deren hauptsächliche Geschäftstätigkeit jedoch nicht einer Einrichtungskategorie gemäß Anlage 1 oder 2 dieses Gesetzes zuzuordnen ist, nicht in unverhältnismäßiger Weise erfasst werden" (Begründung zu § 28 Abs. 3 BSIG-RefE, S. 144). Das oben darstellte weite Begriffsverständnis von "Erbringung ihrer Dienste" läuft diesem Zweck aber gerade zuwider. Diese Frage ist nicht nur für die Reichweite der Pflichten des § 30 BSIG-RefE selbst von zentraler Bedeutung. Dies hat auch weitere Auswirkungen, wie beispielsweise den Umfang der zu erstellenden notwendigen Dokumentation oder die Anordnung von Prüfungen durch Behörden. So sollte auch in den Nachweispflichten nach § 39 deutlich klargestellt sein, dass diese nur den Geltungsbereich der kritischen Anlage umfassen und nicht darüber hinaus gehen. Auch die Beurteilung eines relevanten erheblichen Sicherheitsvorfalls für die Meldepflichten nach § 32 BSIG-RefE wird erleichtert, wenn der Anwendungsbereich klarer, weil enger ist.

Wir empfehlen vor diesem Hintergrund zu prüfen, ob

- **entweder** das Merkmal „Erbringung ihrer Dienste“ auf informationstechnische Systeme, Komponenten und Prozesse, die sie für die Erbringung der Dienste im sektorbezogenen Teilbereich oder zum Betrieb ihrer kritischen Anlage benötigen, beschränkt wird
- **oder** jedenfalls folgende oder eine vergleichbare Klarstellung aufzunehmen, um hinreichend deutlich zum Ausdruck zu bringen, dass die unterschiedliche Risikoexposition und die grundsätzlich geringeren Auswirkungen möglicher Sicherheitsvorfälle außerhalb des sektorbezogenen Teilbereichs zwingend in die Risikobewertung nach § 30 Abs. 1 BSIG-RefE einzubeziehen sind:

  "Vielmehr sind die hier gemeinten Dienste sämtliche Aktivitäten der Einrichtung, für die IT-Systeme eingesetzt werden, dies beinhaltet beispielsweise auch Büro-IT oder andere IT-Systeme, die durch die Einrichtung betrieben werden, aber nicht unmittelbar für die Erbringung ihrer Dienste genutzt werden. Bei der Risikoexposition der Risiken und Auswirkungen eines Ausfalls oder einer Störung solcher IT-Systemen ist die fehlende Unmittelbarkeit besonders zu berücksichtigen."

Durch den Verweis in § 30 Abs. 3 auf Artikel 21 Abs. 5 der NIS-2-Richtlinie (EU) 2022/2555 wird ein Allgefahren-Ansatz angesetzt, bei dem „die Netz- und Informationssysteme und die physische Umwelt dieser Systeme vor Sicherheitsvorfällen zu schützen“ sind. Bestimmte Branchen sind zwar weitestgehend von diesen Anforderungen der europäischen Richtlinie ausgenommen, eine Überlappung gerade im OT-Bereich ist aus unserer Sicht jedoch nicht auszuschließen. Dies erfordert eine Klarstellung im NISUmsuCG, um nicht über die harmonisierten

Anforderungen hinauszugehen und einen erheblichen Mehraufwand für betroffene Unternehmen zu vermeiden.

Außerdem sprechen wir uns dafür aus, dass das Vorschlagsrecht für branchenspezifische Sicherheitsstandards gemäß § 30 Absatz 9 auch auf wichtige Einrichtungen ausgeweitet wird. Mit der Bewährung dieser Möglichkeit durch KRITIS-Betreiber würde solch eine Ausweitung die Vorteile von B3S noch weiter in die Breite tragen, um mehr Einrichtungen aktiv zu beteiligen.

§ 38 Umsetzungs-, Überwachungs- und Schulungspflicht für Geschäftsleitungen besonders wichtiger Einrichtungen und wichtiger Einrichtungen

Die aktuelle Formulierung von § 38 Abs. 1 entsprach bislang der NIS-2-Richtlinie (EU) 2022/2555. Mit dem vierten Referentenentwurf wurde jedoch eine Änderung vorgenommen, indem "Risikomanagementmaßnahmen zu genehmigen" durch "Risikomanagementmaßnahmen umzusetzen" ersetzt wurde. Diese Anpassung ist problematisch, da die Geschäftsführung die Maßnahmen aufgrund fehlender Fachkompetenz im Bereich Informationssicherheit nicht adäquat umsetzen kann. Die Kompetenz hierfür liegt stattdessen bei den entsprechenden Fachabteilungen der betroffenen Unternehmen. Es sollte daher bei der ursprünglichen Formulierung "zu genehmigen" verbleiben. Zusätzlich sollte klargestellt werden, dass die Geschäftsleitung zur Erfüllung der Pflicht nach § 38 Abs. 1 auch Dritte beauftragen kann. Die Letztverantwortung würde bei der Geschäftsleitung bleiben.

§ 41 Untersagung des Einsatzes kritischer Komponenten

Bitkom unterstützt weiterhin das Ansinnen des Gesetzgebers, Kritische Infrastrukturen, soweit technisch und personell möglich, wirksam zu schützen. Schon in unserer Stellungnahme zum IT-Sicherheitsgesetz 2.0 forderten wir, die rechtssichere und hinreichend genaue Definition Kritischer Funktionen, um Kritische Komponenten klar fassen/identifizieren zu können. Es bedarf auch weiterhin einer Liste mit klar formulierten kritischen Komponenten und eindeutig definierten technischen Vorgaben. Diese bzw. Komponenten mit kritischen Funktionen können i. S. dieses Gesetzes nur dann kritisch sein, wenn ihre Funktionalitäten in Bezug auf die Einsatzumgebung im Falle ihrer Beeinträchtigung den KRITIS-Schutzzielen zuwiderlaufen. Spezifikationen erfolgen sektorspezifisch im Rahmen einer Rechtsverordnung unter Beteiligung der betroffenen KRITIS-Sektoren und Betreiber kritischer Anlagen.

§ 54 Zertifizierung

Bitkom begrüßt die Anpassung in § 54 Abs. 8, wonach Sicherheitszertifikate anderer anerkannter Zertifizierungsstellen aus dem Bereich der Europäischen Union vom Bundesamt anerkannt werden können, sofern sie eine Sicherheit aufweisen, die den Sicherheitszertifikaten des Bundesamtes gleichwertig ist und die Gleichwertigkeit vom

Bundesamt festgestellt wurde. Es ist sicherzustellen, dass die Gleichwertigkeit von Sicherheitszertifikaten aller nationalen Zertifizierungsstellen, die heute beispielsweise schon in der SOGIS (Senior Officials Group Information Systems Security) oder auch im „EUCC scheme“ (European Cybersecurity Scheme on Common Criteria) integriert sind, ohne Verzögerung vom Bundesamt festgestellt werden. Die neue Regelung ermöglicht eine koordinierende europäische Zertifizierungslandschaft, trägt zum Gelingen eines digitalen europäischen Binnenmarktes bei und entlastet die Unternehmen bei ihren Zertifizierungsvorhaben. Neue administrative Pflichten, die seitens der Unternehmen bewältigt werden müssen, müssen vermieden werden.

Mit Blick auf § 54 Abs. 5 sollte eine Vermischung von technischen Regeln und Kriterien mit politischen Bewertungen vermieden werden, da ersteres dem Bundesamt und zweiteres dem BMI obliegt. Unnötiger Mehraufwand und Bürokratie sollten vermieden werden. Potenzielle Entscheidungen nach § 54 Abs. 5 müssen frühzeitig und öffentlich durch das Bundesministerium des Innern und für Heimat gegenüber der Industrie und dem Bundesamt angezeigt werden, um Planungs- und Investitionssicherheit zu schaffen.

§ 55 Konformitätsbewertung und Konformitätserklärung

In § 55 des NIS2UmsuCG wird aus unserer Sicht nicht deutlich, welche konkreten Ziele mit der Einführung der Konformitätserklärung verfolgt werden sollen. Auch ist unklar, inwieweit dieser Abschnitt in der NIS-2-Richtlinie (EU) 2022/2555 verankert ist. Die Konformitätsbewertung scheint vielmehr der Einführung des Cyber Resilience Act (CRA) vorzugreifen, was einen isolierten Ansatz innerhalb der EU bedeuten würde.

Um die Ziele der NIS-2-Richtlinie (EU) 2022/2555 zu erreichen, sprechen wir uns daher dafür aus, die Freiwilligkeit der Konformitätsbewertung, ähnlich wie in § 57, für Unternehmen deutlicher zu kennzeichnen.

§ 58 Ermächtigung zum Erlass von Rechtsverordnungen

Durch die explizite Streichung der Verbändeanhörung, insbesondere in § 58, wird eine Rechtsunsicherheit geschaffen. Dies ist nicht im Sinne der Erhöhung der Cybersicherheit der betroffenen Industrie und ihrer Zulieferer. Zwar wird in der zugehörigen Gesetzesbegründung von § 58 auf die GGO verwiesen, dies schafft jedoch weniger Rechtssicherheit als eine Verankerung im NIS2UmsuCG selbst. Wir plädieren daher dafür, die Streichung von „nach Anhörung der betroffenen Wirtschaftsverbände“ zurückzunehmen.

§§ 61/62 Zuständigkeit des Bundesamtes sowie Zentrale Zuständigkeit in der Europäischen Union für bestimmte Einrichtungsarten

§ 61 legt die Zuständigkeit des Bundesamtes für die Einhaltung der Vorschriften aus Teil 3 (§§ 28-50) für wichtige Einrichtungen und besonders wichtige Einrichtungen

sowie für kritische Anlagen in Deutschland fest. Mit § 62 wird diese Zuständigkeit bei IT-Dienstleistungen auf Unternehmensteile oder Beteiligungen in EU-Mitgliedsstaaten erweitert, wenn der Hauptsitz des Unternehmens/Konzerns in Deutschland liegt. Das hätte in der jetzigen Formulierung die Konsequenz, dass das deutsche rechtliche Konzept der „kritischen Anlagen“ auch im europäischen Ausland gelten würde, wenn der Hauptsitz des Betreibers in Deutschland liegt. Dies ist führt zum Export der erhöhten deutschen KRITIS-Anforderungen in das europäische Ausland. Dies gilt es zu vermeiden, weil es über die eigentlichen Anforderungen der NIS2 hinausgeht und in anderen EU-Mitgliedsstatten nicht umsetzbar wäre.

§ 63 Aufsichts- und Durchsetzungsmaßnahmen für besonders wichtige Einrichtungen

Die nach § 65 geschaffenen Untersagungsbefugnisse des BSI gegenüber der Geschäftsführung, des Vorstandes und rechtlichen Vertretern der Unternehmen müssen im Hinblick auf ihre rechtliche Umsetzbarkeit kritisch geprüft werden. Zudem sollten die Haftungsfragen für potenziell verursachte Schäden durch eine Unternehmensübernahme eindeutig geklärt werden.

Artikel 23: Änderungen des Telekommunikationsgesetzes (FNA 900-17)

Für Telekommunikationsunternehmen bleibt es bei einer nicht nachvollziehbaren doppelten Meldepflicht von Vorfällen sowohl an das BSI als auch an die BNetzA (vgl. Artikel 23 § 168 Abs. 1 TKG). Ferner bleibt unklar, warum die Regelung bzgl. der einzuholenden Garantieerklärungen von Herstellern kritischer ITK-Komponenten aufgenommen wurde, obgleich das Bundesministerium des Innern und für Heimat bereits im Oktober 2022 die entsprechende Allgemeinverfügung für den TK-Sektor widerrufen hatte. Diese Ungewissheiten erschweren eine kohärente Umsetzung und schaffen Verwirrung in der Branche.

Zusätzlich könnten wesentliche Änderungen in der Anlage 2 des Sicherheitskataloges (z. B. der Liste der kritischen Funktionen) einen Mehraufwand und ggf. eine Entschleunigung von Innovationen bedeuten. Daher ist es wichtig, mögliche Änderungen am §§165 ff. TKG bei Veröffentlichung genau zu beobachten und zu überprüfen, um potenzielle Auswirkungen auf die Telekommunikationsunternehmen und die Branche insgesamt zu verstehen und angemessen darauf reagieren zu können.

Bitkom vertritt mehr als 2.200 Mitgliedsunternehmen aus der digitalen Wirtschaft. Sie generieren in Deutschland gut 200 Milliarden Euro Umsatz mit digitalen Technologien und Lösungen und beschäftigen mehr als 2 Millionen Menschen. Zu den Mitgliedern zählen mehr als 1.000 Mittelständler, über 500 Startups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Geräte und Bauteile her, sind im Bereich der digitalen Medien tätig, kreieren Content, bieten Plattformen an oder sind in anderer Weise Teil der digitalen Wirtschaft. 82 Prozent der im Bitkom engagierten Unternehmen haben ihren Hauptsitz in Deutschland, weitere 8 Prozent kommen aus dem restlichen Europa und 7 Prozent aus den USA. 3 Prozent stammen aus anderen Regionen der Welt. Bitkom fördert und treibt die digitale Transformation der deutschen Wirtschaft und setzt sich für eine breite gesellschaftliche Teilhabe an den digitalen Entwicklungen ein. Ziel ist es, Deutschland zu einem leistungsfähigen und souveränen Digitalstandort zu machen.

Herausgeber

Bitkom e.V.
Albrechtstr. 10 | 10117 Berlin

Ansprechpartner

Felix Kuhlenkamp | Referent Sicherheitspolitik
T 030 27576-279 | f.kuhlenkamp@bitkom.org

Verantwortliches Bitkom-Gremium

AK Sicherheitspolitik

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
20(4)522

Gesellschaft für Datenschutz
und Datensicherheit e.V.

An die Mitglieder des Innenausschusses
über das Sekretariat des Innenausschusses
innenausschuss@bundestag.de

Stellungnahme der GDD e.V. zum Entwurf der Bundesregierung für ein Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz) - BT-Drs. 20/13184

GDD e.V.
Heinrich-Böll-Ring 10
53119 Bonn
T +49 228 969675-00
F +49 228 969675-25
info@gdd.de
www.gdd.de

1. Art. 1, § 2 BSIG-E (Begriffsdefinitionen)

Im Gesetz werden wesentliche neue Begriffe eingeführt, ohne sie zu definieren.

Der Begriff „Risiko“ ist bislang in den geltenden deutschen Gesetzen nicht definiert! In Art. 6 Nr. 9 der NIS-2-Richtline, in Art. 2 Nr. 6 der CER-Richtlinie sowie in § 2 Abs. 2 Nr. 7 des Referentenentwurfs des KRITIS-Dachgesetzes aus dem April 2024 wird der Begriff dann jedoch definiert. Entweder sollte der Begriff in den jeweiligen Umsetzungsgesetzen konsequent nicht legaldefiniert werden oder in allen neuen Gesetzen, die ihn verwenden. Es wird daher empfohlen eine entsprechende Definition in den BSIG-E aufzunehmen:

> *„Risiko“ das Potenzial für Verluste oder Störungen, die durch einen Sicherheitsvorfall verursacht werden, das als eine Kombination des Ausmaßes eines Verlusts oder einer Störung und der Wahrscheinlichkeit des Eintretens des Sicherheitsvorfalls zum Ausdruck gebracht wird;*

Entsprechend sollte der Begriff „Risikoanalyse“ analog zum § 2 Nr. 7 KRITIS-Dachgesetz definiert werden:

> „Risikoanalyse“ ein systematisches Verfahren zur Bestimmung eines Risikos;

Die NIS-2-Richtlinie nutzt an mehreren Stellen den Begriff „Cyberhygiene“ (z.B. Art. 7 Abs. 1 lit. f) und i, Art. 21 Abs. 2 lit. g) ohne ihn zu definieren. In § 30 Abs. 2 Nr. 7 BSIG-E und im Art. 17, § 5c Abs. 3 Nr. 7 neu EnWG wird der neue Begriff „Cyberhygiene“ auch verwendet. Im Art. 26, § 165 Abs. 2a Nr. 7 neu TKG wird in der Formulierung darauf verzichtet. Im Interesse einer Einheitlichkeit sollte der Begriff an allen drei Stellen des Gesetzentwurfs benutzt werden oder einheitlich die Formulierung aus dem TKG-E genutzt werden.

Die Erläuterungen in der Begründung auf Seite 139 in Abs. 2 zeigen, dass der Begriff erläutert werden muss. Deshalb sollte der Begriff „Cyberhygiene“, falls er verwendet wird, eine Legaldefinition erhalten. Ausgehend von der Begründung wäre die folgende Definition möglich:

> *„Cyberhygiene“ die Anwendung grundlegender Verfahren und Herangehensweisen, welche allgemein zu einer Verbesserung des Cybersicherheitsniveaus einer Einrichtung führen. Dies umfasst gegebenenfalls unter anderem ein Patchmanagement, Regelungen für sichere Passwörter, die Einschränkung von Zugriffskonten auf Administratorenebene, Netzwerksegmentierungen, Schutz vor Schadsoftware sowie Backup- und Sicherungskonzepte für Daten.*

An dieser Stelle sei noch angemerkt, dass der Entwurf die Begriffe Informationssicherheit (Definition § 2 Nr. 17 BSIG-E), Datensicherheit (§ 20 Abs. 3 Nr. 1 BSIG-E), Netzsicherheit (§ 20 Abs. 3 Nr. 1 BSIG-E), Netz- und Informationssicherheit (z.B. § 23 Abs. 2 lit. a)), IT-Sicherheit (z.B. § 15 und im Kontext des IT-Sicherheitskennzeichen im BSIG-E oder Art 17 § 5c neu EnWG), Cybersicherheit (im Kontext von Zertifizierung, z.B. § 3 Nr. 9 BSIG-E) oder Sicherheit in der Informationstechnik (Definition § 2 Nr. 39 BSIG-E) verwendet, ohne dass immer der Unterschied der Bedeutung erkennbar wird. Der Entwurf sollte auf eine einheitliche, stringente Verwendung der Begriffe geprüft werden. Einheitliche Begriffe tragen letztendlich auch zur Verständlichkeit und Rechtssicherheit bei Experten und Bürgern bei.

2. Art. 1, § 1 BSIG-E (Aufgabenmaßstab)

Im Rahmen des 2. IT-Sicherheitsgesetzes (IT-SiG 2.0) wurde in § 1 die Regelung eingeführt, dass das Bundesamt für Sicherheit in der Informationstechnik (BSI) seine Aufgaben gegenüber den Bundesministerien auf Grundlage wissenschaftlich-technischer Erkenntnisse durchführt. Die entsprechende Formulierung findet sich nun auch in § 1 BSIG-E wieder. Sie wirft jedoch die Frage auf, was der erkenntnisleitende Maßstab der Arbeit des BSI gegenüber seinen übrigen Zielgruppen (Bundesbehörden, Verbraucher, Hersteller, Anwender etc.) sein soll. Sollen die diese Zielgruppen betreffenden Aufgaben nach politischen, wirtschaftlichen oder sonstigen Maßgaben durchgeführt werden? An dieser Stelle wäre eine Klarstellung sinnvoll.

3. Art. 1, § 3 Abs. 1 S. 2 Nr. 18 c BSIG-E (Unterstützung der Sicherheitsbehörden)

Bereits seit vielen Jahren ist in der Aufgabennorm des BSI die Unterstützung verschiedenster Sicherheitsbehörden vorgesehen. Dazu findet sich die Einschränkung: „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.“. Insbesondere der hintere Satzteil vermag jedoch Zweifel zu schüren, ob das BSI zweifelsfrei der IT-Sicherheit verpflichtet ist oder es nicht doch auch zu seinem Aufgabenprofil gehört, den übrigen Sicherheitsbehörden bei der Ausnutzung

von IT-Unsicherheit zu helfen. Während diese Unklarheit früher noch dadurch gerechtfertigt werden konnte, dass das BSI die vorrangige und kompetente Stelle des Bundes in Fragen der Informationstechnik war, hat sich die Lage inzwischen verändert. Genau für diese Beratungsaufgaben gegenüber den Sicherheitsbehörden wurde 2017 die Zentrale Stelle für Informationstechnik im Sicherheitsbereich (ZITiS) als Bundesüberbehörde gegründet. Damit besteht kein Grund mehr, dass das BSI anderen Interessen gegenüber verpflichtet bleibt als denen der IT-Sicherheit. Der Satzteil „oder unter Nutzung der Informationstechnik erfolgen" sollte daher gestrichen werden

4. Art. 1, § 5 BSIG-E (Schwachstelleninformationen)

Wie bisher soll das BSI als zentrale Meldestelle Informationen über Sicherheitsrisiken, zu denen auch Informationen über Sicherheitslücken in Hard- und Software gehören, entgegennehmen (Abs. 1 und 2). Diese Informationen sollen unter anderem genutzt werden, um Dritte über die Schwachstellen zu informieren (Abs. 3). Das BSI soll also als Informationsdrehscheibe für IT-Sicherheitslücken dienen.

Wir begrüßen grundsätzlich, dass mit dem BSI ein zentraler Ansprechpartner für entdeckte IT-Sicherheitslücken festgelegt wird. Allerdings befindet sich das BSI ebenso wie die Polizeien und das Bundesamt für Verfassungsschutz im Geschäftsbereich des Bundesministeriums des Innern und für Heimat (BMI). Diese anderen Sicherheitsbehörden haben ein Interesse daran, dass Sicherheitslücken zwar ihnen bekannt aber nicht geschlossen werden, damit sie diese etwa für Remote Forensic Software ausnutzen können. Da das BSI gegenüber dem BMI weisungsgebunden ist, kann auf Basis des aktuellen Gesetzestextes nicht ausgeschlossen werden, dass das BSI angewiesen wird, eine ihm gemeldete Sicherheitslücke zurückzuhalten, statt den Hersteller zu informieren und die Anwender zu warnen. Angesichts der Bedeutung, den eine verlässlich sichere Informationstechnik für die digitalisierte Gesellschaft hat, ist dieses Risiko nicht akzeptabel. Wenn dem BSI Lücken bekannt werden, müssen diese dem Hersteller gemeldet werden, damit dieser sie schließen kann. Nur so können die Anwender in die Lage versetzt werden, ihre IT sicher zu betreiben und damit die Ziele der NIS-2-Richtlinie zu erreichen.

Daher sollte im Gesetz klargestellt werden, dass das BSI die ihm bekannt gewordenen Sicherheitslücken stets dem Hersteller legitimer Software zu melden hat und entgegenstehende Weisungen nicht zu befolgen braucht. Hierfür könnten nach Abs. 3 S. 1 Nr. 5 eine neue Nr. 6 und ein Abs. 3 S. 2 und S. 3 ergänzt werden:

„6. Hersteller von Hard- und Software über Schwachstellen in ihren Produkten zu informieren.

Weisungen des Bundesministeriums des Innern und für Heimat, die von S. 1 Nr. 6 abweichen, nimmt das BSI nicht entgegen. Eine Abweichung von S. 1 Nr. 6 ist nur zulässig, wenn es sich bei dem Produkt selbst um Schadsoftware handelt."

Damit wird ausgeschlossen, dass dem BSI Weisungen erteilt werden können, die einer Schwachstellenschließung und damit einer sicheren IT-Infrastruktur in Deutschland entgegenstehen. Der neue Abs. 3 S. 3 stellt klar, dass Hersteller von Schadsoftware selbstverständlich nicht über Lücken in ihrer Software nicht informiert werden müssen.

5. Art. 1, § 7 Abs. 6 und 7 BSIG, § 29 Abs. 3 BSIG-E, § 43 Abs. 5 S. 4 BSIG, § 44 Abs. 1 S. 5 und Abs. 6 S. 3 BSIG-E

Der vorgelegte Gesetzentwurf sieht eine ganze Reihe von Ausnahmen für bestimmte Behörden vor. Dazu zählen etwa die Ausnahmen für die Auslands-IT des Auswärtigen Amtes sowie den Geschäftsbereich des Bundesministeriums der Verteidigung im Zusammenhang mit Kontrollbefugnissen des BSI. Auch im Zusammenhang mit den Absicherungs- und Meldepflichten finden sich Ausnahmen für beide Ressorts und zusätzlich den BND und das BfV.

Das ist insofern unverständlich, da die IT der Bundesverwaltung vernetzt ist und jedes Netz nur so sicher ist, wie sein schwächstes Glied. Zudem erscheint es vor dem Hintergrund der Zeitenwende, verstärkter Aufklärungs-Aktivitäten und Cyberoperationen fremder Staaten kaum nachvollziehbar, dass gerade die IT-Sicherheit dieser wichtigen Bereiche gesetzlich von gesetzlichen Pflichten ausgenommen und der Eigenverantwortung der jeweiligen Einrichtung überlassen werden sollen. Gerade im Hinblick auf die erfolgreichen und öffentlich gewordenen Angriffe auf das Auswärtige Amt haben gezeigt, dass in diesem Bereich Handlungsbedarf besteht. Daher sollten sämtliche Ausnahmen für einzelne Teile der Bundesverwaltung gänzlich gestrichen werden. Es ist nicht konsequent, einerseits der Wirtschaft mit Verweis auf die gewachsene Gefährdungslage und die Folgen eines Ausfalls von Unternehmen immer mehr Pflichten in Bezug auf die Informationssicherheit aufzuerlegen und andererseits wichtige Teile der öffentlichen Verwaltung von entsprechend engen Verpflichtungen auszunehmen.

6. Art. 1, § 30 Abs.1 BSIG-E, Art. 17, § 5c Abs. 3 neu EnWG und Art. 25, § 165 Abs. 2a neu TKG

In diesen drei Änderungen wird eine Aufzählung von Vorgaben aus Art. 21 Abs. 2 der NIS-2-Richtlinie umgesetzt. Dabei wird nicht auf einheitliche Begriffe gesetzt. In der jeweiligen Nr. 1 wird nebeneinander „Sicherheit in der Informationstechnik“ (BSIG-E), „Sicherheit für Informationstechnik“ (EnwG) und „Sicherheit für Informationssysteme“ (TKG) genutzt. In der jeweiligen Nr. 5 wird „informationstechnischen Systemen, Komponenten und Prozessen“ (BSIG-E) und „Netz- und Informationssystemen“ (EnWG und TKG) verwendet.

Wenn schon bei der erstmaligen Umsetzung unterschiedliche Formulierungen für identische Sachverhalte genutzt werden, lässt sich absehen, wie die Formulierungen nach einigen Gesetzes-Novellen auseinanderlaufen. Die IT-Sicherheitsgesetzgebung benötigt jedoch einheitliche und sauber definierte Begriffe.

7. Art. 1, § 31 Abs. 2 BSIG-E (Systeme zur Angriffserkennung)

Die Regelung des § 31 Abs. 2 BSIG-E heben eine bestimmte Risikomanagementmaßnahme, nämlich die Angriffserkennungssysteme, heraus, ohne dass ersichtlich ist, warum. Welche Risikomanagementmaßnahmen zu ergreifen sind, muss sich immer aus einer vorausgehenden Risikoanalyse ergeben. Erst aus dieser lässt sich ableiten, welche Maßnahmen das Risiko am effektivsten adressieren. Angriffserkennungssysteme können eine dieser Maßnahmen sein. Ob sie jedoch die sind, die in einer Auswahl verschiedener Maßnahmen und unter Berücksichtigung des Aufwandes insgesamt den besten Schutz versprechen, lässt sich nicht a priori und für alle Fälle gleichförmig beantworten. Es ist denkbar, dass die Aufwände für den Aufbau und Betrieb eines Angriffserkennungssystems in anderen Maßnahmen besser investiert wären und zu einem höheren Schutzniveau führen. Auf dieses grundsätzliche Problem wurde bereits bei Einführung der Vorgängerregelung durch IT-Sicherheitsexperten hingewiesen. Leider wurde dem kein Gehör geschenkt. Wenn Ziel des Gesetzes ist, die IT-Sicherheit bestmöglich zu fördern, sollte dieser Fehler nicht fortgeschrieben, sondern § 31 Abs. 2 BSIG-E gestrichen werden.

8. Art. 1, §§ 32, 40 BSIG-E (Meldepflichten)

a. Mit § 32 BSIG-E wird eine große Zahl von Einrichtungen einer neuen Meldepflicht unterworfen. Dabei unterliegen bereits heute viele Unternehmen verschiedensten Meldepflichten aufgrund verschiedenster Regelungen. Dazu zählt u.a. die Meldepflicht für Datenschutzverletzungen nach Art. 33 DS-GVO. Die Vielzahl unterschiedlicher Meldeverpflichtungen führt zu einem kontinuierlichen Anstieg der Bürokratie für die verpflichteten Einrichtungen, ohne dass dem im gleichen Maß Vorteile gegenüberstehen. Daher sollte bereits auf gesetzgeberischer Ebene versucht werden, die Meldepflichten zu vereinfachen und zu vereinheitlichen. Hier gilt es die Möglichkeiten, die die Digitalisierung der Verwaltung bietet, zu nutzen.

Gerade im Fall von IT-Sicherheitsvorfällen ist die Wahrscheinlichkeit hoch, dass auch personenbezogene Daten betroffen sein können und neben der Meldepflicht nach NIS-2 auch eine nach Art. 33 DS-GVO ausgelöst wird. Statt zweimal an unterschiedliche Stellen melden zu müssen, wäre es sinnvoll, ein zentrales Meldeportal zu etablieren, auf dem die Meldepflichtigen ihre Informationen einmal zentral eingeben und das dann automatisch die jeweils benötigten Eingaben an die jeweils zuständige NIS-2- und Datenschutzaufsichtsbehörde weiterleitet.

Der Bundesrat hatte bereits einen entsprechenden Vorschlag unterbreitet (BR-Drs. 380/24, S. 11). Auch wenn dieser Vorschlag noch nicht ausgereift war, begrüßen wir das dahinterstehende Ziel, den Meldeaufwand für die Einrichtungen zu reduzieren. Da die Realisierung weder rechtlich noch in der technischen Umsetzung trivial ist und die gesetzgeberische Lösung sicherlich einige Zeit benötigt, ist es aus Sicht der GDD nachvollziehbar, diesen Vorschlag noch nicht im laufenden NIS-2-Umsetzungsgesetzgebungsverfahren aufzugreifen. Dies würde die ohnehin

verspätete Richtlinienumsetzung nur noch weiter verzögern. Gleichwohl bitten wir den Ausschuss, diese vereinheitlichte Meldemöglichkeit weiter zu verfolgen, ausarbeiten zu lassen und bei passender Gelegenheit in ein Gesetzgebungsverfahren einzubringen, um den Erfüllungsaufwand in der Wirtschaft jedenfalls mittelfristig wieder zu reduzieren.

b. Die Meldepflicht wird durch „erhebliche Sicherheitsvorfälle“ ausgelöst. Der Begriff wird zwar in § 2 Nr. 11 BSIG-E definiert, diese Definition wird jedoch praktische Folgefragen auf. Denn ein Sicherheitsvorfall soll auch dann erheblich sein, wenn er andere Personen „durch erhebliche materielle oder immaterielle Schäden beeinträchtigt hat oder beeinträchtigen kann“. Es bleibt unscharf, was erhebliche immaterielle Schäden sein sollen. Die nähere gesetzliche Vorkonturierung ist insbesondere deswegen nötig, da bereits die Möglichkeit solcher Schäden die Meldepflicht auslösen sollen und Verstöße gegen die Meldepflicht bußgeldbewehrt sind. Für die verpflichteten Einrichtungen muss hier Rechtsklarheit geschaffen werden.

9. Art. 1, § 50 Abs. 1 BSIG-E (Auskünfte Domainnamen)

§ 50 Abs. 1 BSIG-E verpflichtet Top-Level-Domain Name Registries und Domain-Name-Registry-Dienstleister zur Herausgabe der bei ihnen gespeicherten Informationen auf berechtigtes Verlangen. Die Informationen sollen binnen 72h herausgegeben werden und das Nichtvorliegen der Informationen soll sogar binnen 24h nach Antragseingang mitgeteilt werden.

Damit wirft die Regelung zwei Probleme auf. Das erste ist die Frage, wann ein Informationsverlangen berechtigt ist. Dazu geben weder der Wortlaut der Richtlinie noch der vorliegende Umsetzungsgesetzestext einen Hinweis. Im Hinblick darauf, dass es sich bei den herauszugebenden Informationen um personenbezogene Daten handeln kann, erscheint eine Herausgabepflicht ohne klar umrissenen Verarbeitungszweck und Berechtigungsumfang problematisch. Hier ist eine klarere Konturierung der Pflicht im Gesetzestext selbst notwendig.

Das zweite Problem ergibt sich aus der Frist für Negativmitteilungen von 24h. Es ist ohnehin problematisch, wenn zu Negativmitteilungen verpflichtet wird, da diese für die Unternehmen stets unnötige Aufwände erzeugen. Warum dann die Pflicht auch noch binnen 24h – für die Unternehmen also prioritär – erfüllt werden soll, ist nicht nachvollziehbar. Die Richtlinie selbst schreibt für die Auskunft selbst vor, dass diese zwar unverzüglich aber spätestens binnen 72h zu beantworten sind. Damit erfasst sie sowohl die Positiv- wie die Negativantwort in einer einheitlichen Frist. Daran sollte sich auch die deutsche Umsetzung orientieren, statt ohne Not über die Richtlinienvorgaben hinauszugehen.

10. Art. 1, § 65 BSIG-E (Bußgeldvorschriften)

In § 65 Abs. 10 BSIG-E wird – ganz der Richtlinie folgend – geregelt, dass das BSI als NIS-2-Aufsichtsbehörde dann keine Bußgelder verhängen darf, wenn die

Datenschutzaufsichtsbehörden für das gleiche Verhalten bereits eine nach Art. 58 DS-GVO verhängt haben.

Wir begrüßen, dass der europäische und der deutsche Gesetzgeber eine Doppelsanktionierung von Verstößen gegen die Datensicherheit im Cybersicherheits- und Datenschutzrecht vermeiden wollen. Leider ist die Regelung weder auf europäischer noch auf nationaler Ebene gelungen, da sie lediglich der NIS-2-Behörde verbietet, ein Bußgeld zu verhängen, wenn die Datenschutzbehörde dies bereits getan hat. Umgekehrt ist die Verhängung eines Bußgeldes durch die Datenschutzaufsichtsbehörden aber weiterhin möglich, wenn die NIS-2-Behörde bereits eines für das gleiche Verhalten verhängt hat. Es ist nach den derzeitigen Regelungen also vom Zufall bzw. der Geschwindigkeit der jeweiligen Behörden abhängig, ob einer Einrichtung eine Doppelbestrafung droht oder nicht. Stattdessen sollte aber das Bußgeldverfahren gesetzlich so strukturiert werden, dass Doppelsanktionen sicher ausgeschlossen sind. Da eine Einschränkung der Bußgeldkompetenz der Datenschutzbehörden europarechtlich ausgeschlossen ist, wäre es etwa denkbar, dass das BSI als NIS-2-Bußgeldbehörde vor Einleitung eines Bußgeldverfahrens das Einvernehmen der zuständigen Datenschutzaufsichtsbehörde einholen muss. Diese könnte mit dem Einvernehmen erklären, selbst nicht wegen des gleichen Verhaltens ein Bußgeld nach der DS-GVO verhängen zu wollen. Die jeweils zuständige Datenschutzaufsichtsbehörde ist dem BSI aufgrund der Angaben aus der Registrierung der Einrichtungen auch bereits bekannt.

Die entsprechende Vorgabe könnte durch eine Ergänzung des § 65 Abs. 1 BSIG-E um folgenden Satz erreicht werden:

„Um eine doppelte Verhängung von Bußgeldern zu vermeiden, hat das Bundesamt vor Verhängung eines Bußgeldes das Einvernehmen der zuständigen Aufsichtsbehörde nach der Verordnung (EU) 2016/679 einzuholen.“

11. Art. 7 (Änderung des Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme)

Mit Art. 7 NIS2UmsuCG soll die in Art. 6 des zweiten IT-Sicherheitsgesetzes (IT-SiG 2.0) enthaltene Evaluierungsklausel aufgehoben werden. Diese verpflichtet das BMI dazu, die mit dem IT-SiG 2.0 eingeführten Regelungen, u.a. im BSIG, bis zum Mai 2025 zu evaluieren. Die Streichung wird damit begründet, dass sich viele der damals enthaltenen Vorschriften durch die NIS-2-Umsetzung ändern und die unveränderten Regelungen durch das NIS2UmsuCG bestätigt würden. Das überzeugt jedoch nicht. Denn eine Evaluierung dient nicht der bloßen Bestätigung existierender Regelungen. Vielmehr dient sie der Überprüfung, ob die mit einem Gesetz verfolgten Ziele durch die Regelungen auch in der Praxis erreicht werden oder Anpassungen notwendig sind. Eine Evaluierung ist die erforderliche Grundlage dafür, gesetzliche Regelungen entweder zu bestätigen oder anzupassen. An einer solchen Grundlage fehlt es für die im BSIG enthaltenen Grundlagen weiterhin. Denn bereits mit Art. 6 IT-SiG 2.0 wurde die zuvor im IT-Sicherheitsgesetz von 2015 vorgesehen Evaluierungspflicht aufgehoben. Es drängt sich daher der

Eindruck auf, dass zwar entsprechend Klauseln immer wieder vorgesehen, die Evaluierungen dann aber nicht durchgeführt, sondern die Klauseln bei nächster Gelegenheit lieber wieder gestrichen werden. Das ist nicht akzeptabel, da die eingeführten Verpflichtungen für die Unternehmen massive Aufwände erzeugen und deren Wirksamkeit daher regelmäßig überprüft werden sollten, um ein angemessenes Verhältnis von Aufwand und Wirkung sicherzustellen. Auch im Hinblick auf die dem BSI seit 2015 eingeräumten Eingriffsbefugnisse und deren grundrechtseinschränkende Wirkung ist eine Evaluierung inzwischen dringend geboten.

12. Verpflichtungen der Länder- und Kommunalverwaltungen

Zum Abschluss möchten wir noch einmal darauf hinweisen, dass auch die Landes- und Kommunalverwaltung entsprechenden IT-Sicherheitspflichten unterworfen werden muss. Bereits in der Vergangenheit haben wir uns dem dahingehenden offenen Brief des TeleTrust e.V. angeschlossen. Die letzten Jahre haben gezeigt, wie verwundbar die IT-Infrastrukturen sind, auf die alle Bürgerinnen und Bürger angewiesen sind. Die Auswirkungen der Vorfälle in Anhalt-Bitterfeld sowie bei der Südwestfalen-IT haben gezeigt, dass gerade dort die IT-Strukturen besonders anfällig sind, wo Bürgerinnen und Bürger den intensivsten Kontakt mit dem Staat haben. Das darf nicht so bleiben! Es muss leider davon ausgegangen werden, dass sich an diesem Zustand ohne gesetzliche Verpflichtungen nichts ändern wird. Auch wenn der Bundestag nicht die notwendige Gesetzgebungskompetenz besitzt, fordern wir seine Mitglieder auf, sich bei ihren (Partei-)Kolleginnen und Kollegen auf Landesebene für entsprechende Gesetzgebungsmaßnahmen einzusetzen. In Zeiten kriegerischer Auseinandersetzungen, die auch im Cyberraum ausgetragen werden, hängt davon die Funktionsfähigkeit unseres Staates und unserer Gesellschaft ab.

Bonn, den 29.10.2024

Die Gesellschaft für Datenschutz und Datensicherheit e.V. (GDD) tritt als gemeinnütziger Verein für einen sinnvollen, vertretbaren und technisch realisierbaren Datenschutz ein. Sie hat zum Ziel, die Daten verarbeitenden Stellen - insbesondere auch die Datenschutzbeauftragten - bei der Lösung und Umsetzung der vielfältigen mit Datenschutz und Datensicherheit verbundenen rechtlichen, technischen und organisatorischen Anforderungen zu unterstützen.

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
20(4)524

Stellungnahme

des Gesamtverbandes der
Deutschen Versicherungswirtschaft
Lobbyregister-Nr. R000774

zum Gesetzentwurf der Bundesregierung:
Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz)

BT-Drucksache 20/13184

Inhalt

Gesamtverband der Deutschen Versicherungswirtschaft e. V.
Wilhelmstraße 43 / 43 G, 10117 Berlin
Postfach 08 02 64, D-10002 Berlin
Telefon: +49 30 2020-5000 · Telefax: +49 30 2020-6000
Lobbyregister-Nr. R000774

Rue du Champ de Mars 23, B-1050 Brüssel
Telefon: +32 2 28247-30 · Telefax: +49 30 2020-6140
ID-Nummer 6437280268-55
www.gdv.de

Ansprechpartner
Betriebswirtschaft, IT und Prozesse

E-Mail
bdit@gdv.de

1. Zusammenfassung

Die deutsche Versicherungswirtschaft begrüßt das Vorhaben der Bundesregierung, die Cyberresilienz in Deutschland weiter zu stärken. Auch wenn Versicherungsunternehmen von der nationalen Umsetzung der NIS-2-Richtlinie grundsätzlich nicht erfasst sind, besteht weiterhin die Gefahr einer Doppelregulierung.

Dies betrifft Teile der Versicherungskonzernstruktur (hier: gruppeninterne IT-Töchter), die weiterhin in den Anwendungsbereich fallen sollen. Wir regen daher an, dass gruppeninterne IT-Töchter konsequenterweise

- entweder komplett ausgenommen werden (siehe 2.1) oder
- zumindest eine Gleichbehandlung der kleinen und großen IT-Töchter (siehe 2.2) umgesetzt wird.

2. Einleitung

Durch den Digital Operational Resilience Act (DORA: Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die digitale operationale Resilienz im Finanzsektor) unterliegen Versicherungsunternehmen bereits umfassenden Vorgaben bzgl. der weiteren Stärkung der Cybersicherheit – z. B. Melde- und Nachweispflichten. Zur Vermeidung von Doppelregulierung hat der Europäische Gesetzgeber daher eine lex-specialis-Regelung in DORA aufgenommen. Die Versicherungsunternehmen sollen als Finanzunternehmen im Sinne von Artikel 2 Absatz 2 der DORA-Verordnung entsprechend von NIS-2 ausgenommen sein.

Allerdings gilt dies nach dem definierten Anwendungsbereich nicht für deren gruppeninterne IT-Töchter. Wenn diese jedoch ausschließlich für eines bzw. mehrere der aus dem Anwendungsbereich ausgenommenen Versicherungsunternehmen IKT-Dienstleistungen erbringen, ist eine Regulierung über das NIS-2-Umsetzungsgesetz neben DORA nicht erforderlich. Zur Orientierung kann die Regelung des Artikel 31 Abs. 8 lit. iii) DORA-VO dienen, wonach gruppeninterne IKT-Dienstleister nicht als kritische IKT-Drittdienstleister anzusehen sind.

2.1 Zu § 28 NIS-2-Umsetzunggesetz (Besonders wichtige und wichtige Einrichtungen): Besonderheit der unternehmenseigenen bzw. gruppeninternen IT-Dienstleister in der Versicherungswirtschaft

Im Regierungsentwurf zum NIS-2-Umsetzungsgesetz werden in Kapitel 1 „Anwendungsbereich“ in § 28 Abs. 5 (Besonders wichtige Einrichtungen und wichtige Einrichtungen) Finanzunternehmen und damit im Ergebnis die Versicherungswirtschaft über die Nennung von DORA als lex specialis ausgenommen.

Der hier einschlägig zitierte Artikel 2 Abs. 2 DORA benennt die in Art. 2 Abs.1 lit. a) bis t) DORA aufgeführten Unternehmen als Finanzunternehmen, für die alle Bestimmungen aus DORA gelten. In diesem Artikel ausgenommen sind die in Artikel 2 Abs. 1 lit. u) DORA genannten IKT-Drittanbieterdienstleister. Sinnvoll wäre hier eine Ausnahme für alle IKT-Drittdienstleister des Finanzsektors, die ausschließlich gruppenintern tätig sind. Diese Wertung entspräche auch dem Verständnis des Europäischen Gesetzgebers, der gruppeninterne IKT-Drittdienstleister von dem Überwachungsrahmen für kritische IKT-Drittanbieter nach DORA ausnimmt (Art. 31 Abs.8 lit. iii) DORA). Dies trägt dem Umstand Rechnung, dass die stark regulierten Finanzunternehmen regelmäßig größeren Einfluss auf die gruppeninternen IT-Dienstleister haben und die Einhaltung der strengen Sicherheitsanforderungen bereits hinreichend überwachen.

Wir regen daher weiterhin die Streichung der gruppeninternen IT-Dienstleister aus dem Anwendungsbereich des NIS-2-Umsetzungsgesetzes an:

§28 Abs (5) Die §§ 30, 31, 32, 35, 36, 38 und 39 gelten nicht für
1. Finanzunternehmen nach Artikel 2 Absatz 2 der Verordnung (EU) 2022/2554 und Unternehmen, für welche die Anforderungen der Verordnung (EU) 2022/2554 auf Grund von § 1a Absatz 2 Kreditwesengesetz oder § 293 Absatz 5 Versicherungsaufsichtsgesetz gelten, ***sowie deren gruppeninterne IKT-Dienstleister****.*

2.2 Zu § 28 Absatz 6 NIS-2-Umsetzungsgesetz (Besonders wichtige und wichtige Einrichtungen): Ausnahmeregelung

§ 28 Abs. 6 NIS-2-Umsetzunggesetz nimmt Nicht-Finanzunternehmen, die Betreiber kritischer Anlagen sind, von den Meldepflichten nach § 32 NIS-2-Umsetzunggesetz aus, soweit sie Anlagen für Finanzunternehmen betreiben.

Das ist sinnvoll, damit bei Sicherheitsvorfällen nicht ein doppelter Meldeaufwand betrieben werden muss. Nach der DORA-VO (vgl. Art. 28 Abs. 1 lit. a DORA) bleiben Finanzunternehmen auch bei Auslagerung auf IKT-Drittdienstleister für die Erfüllung der Anforderungen der DORA-VO voll verantwortlich. Zu diesen Anforderungen gehören auch die in Art. 19 Abs. 4 DORA-VO abgestuften Meldepflichten. Finanzunternehmen müssen also auch Sicherheitsvorfälle melden, die bei Anlagen auftreten, die für sie durch einen Dienstleister betrieben werden.

Die DORA-VO unterscheidet aber nicht wie das NIS-2-Umsetzunggesetz zwischen „Betreibern kritischer Anlagen“ und „besonders wichtigen Einrichtungen“ sowie „wichtigen Einrichtungen“.

Dies hat zur Folge, dass für die beiden niedrigeren Gefährdungskategorien eine gesteigerte, weil doppelte Meldepflicht entsteht:

- Nicht-Finanzunternehmen, die Betreiber kritischer Anlagen sind und diese Anlagen für Finanzunternehmen betreiben, müssen richtigerweise nicht nach NIS-2-Umsetzungsgesetz melden, weil das Finanzunternehmen nach DORA meldet.

- Nicht-Finanzunternehmen, die „nur“ besonders wichtige oder wichtige Einrichtungen sind und Anlagen für Finanzunternehmen betreiben, müssen dagegen nach NIS-2-Umsetzungsgesetz melden, obwohl das Finanzunternehmen bereits nach DORA meldet.

Wir regen daher an, die Ausnahme aller gruppeninternen IT-Dienstleister aus den in §32 hinterlegten Meldepflichten des NIS-2-Umsetzungsgesetzes durch folgende Ergänzung des §28 Abs. 6 umzusetzen:

(6) § 32 gilt nicht für Betreiber kritischer Anlagen ***sowie besonders wichtige Einrichtungen und wichtige Einrichtungen****, soweit sie eine Anlage für Unternehmen nach Absatz 5 Nummer 1 betreiben.*

Berlin, den 31.10.2024

Deutscher Bundestag

Ausschuss für Inneres und Heimat

Ausschussdrucksache
20(4)528

AG KRITIS

Arbeitsgruppe Kritische Infrastrukturen

Stellungnahme zum Regierungsentwurf des NIS2UmsuCG vom 02.10.2024

Version 1.1 – zuletzt editiert am 27.10.2024

1 Arbeitsgruppe Kritische Infrastrukturen

Dieses Dokument wurde von Mitgliedern der unabhängigen Arbeitsgruppe Kritische Infrastrukturen (AG KRITIS) erstellt.

Wir haben uns im Frühjahr 2018 erstmals zusammengefunden, um Ideen und Anregungen zur Erhöhung der Resilienz und Sicherheit kritischer Dienstleistungen von Betreibern kritischer Infrastrukturen im Sinne des Gemeinwohls zu entwickeln. Unser Ziel ist es, die Versorgungssicherheit der deutschen Bevölkerung zu erhöhen, indem wir die Bewältigungskapazitäten des Staates zur Bewältigung von Großschadenslagen, die durch Cyberangriffe hervorgerufen wurden, ergänzen und erweitern wollen. Unsere Arbeitsgruppe ist unabhängig von Staat, Verwaltung oder wirtschaftlichen Interessen.

Die AG KRITIS besteht aus ca. 42 Fachleuten und Experten, die sich mit Kritischen Infrastrukturen (KRITIS) gemäß § 2 (Abs 10) BSI-Gesetz [1] und gemäß § 10 BSIG zugehöriger *Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz* [2] (BSI-Kritisverordnung - BSI-KritisV) beruflich beschäftigen, zum Beispiel durch Planung, Aufbau, Betrieb sowie Beratung, Forschung oder Prüfung der beteiligten Systeme und Anlagen. Unser Engagement ist getrieben von der Motivation, unabhängig von wirtschaftlichen Interessen eine nachhaltige Verbesserung der Sicherheit jener Anlagen kooperativ mit allen Beteiligten herbeizuführen und damit im Katastrophenfall die öffentliche Sicherheit zu verbessern. Wir sind kein Wirtschaftsverband oder Unternehmen und haben daher auch und insbesondere keine Sponsoren.

Uns eint, dass wir durch unsere Arbeit unabhängig voneinander zu dem Schluss gekommen sind, dass die Ressourcen der Bundesrepublik Deutschland zur Bewältigung von Großschadenslagen auf Grund von informations- und operationstechnischen Vorfällen im Bereich der Kritischen Infrastrukturen nicht ausreichen. In der Folge sind resultierende Krisen oder Katastrophen nicht oder kaum zu bewältigen. Es sollen daher Wege gefunden werden, das Eintreten gravierender Folgen dieser Vorfälle durch schnelles und kompetentes Handeln zu verhindern oder zumindest abzuschwächen und eine Regelversorgung in kürzest möglicher Zeit wieder sicherzustellen.

[1] www.gesetze-im-internet.de/bsig_2009/BJNR282110009.html
[2] www.gesetze-im-internet.de/bsi-kritisv/BJNR095800016.html

2 Stellungnahme

Mit dem vorliegenden Referentenentwurf (Gesetzentwurf der Bundesregierung, Drucksache 20/13184) des *Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz)*, kurz NIS2UmsuCG, wird die Umsetzung der EU NIS2-Richtlinie (2022/2555) angestrebt. Damit einher geht eine Ausweitung des Geltungsbereiches von Betreibern kritischer Anlagen (ehem. sogenannte KRITIS-Betreiber) und der als wichtige und besonders wichtige Einrichtungen definierten sonstigen Unternehmen.

Das NIS2UmsuCG ist ein Artikelgesetz, welches insgesamt über 23 Gesetze und Verordnungen ändern soll. Unsere Kommentierung bezieht sich hierbei ausschließlich auf die unter Artikel 1 eingebrachte Änderung des BSI-Gesetzes.

Mit dem neuen Referentenentwurf vom 02.10.2024 werden aus unserer Sicht keine wesentlichen Verbesserungen zu den bisherigen Referentenentwürfen erreicht und lediglich **Defizite** aufrechtgehalten:

- § 15 (1): Einschränkung auf **bekannte** Schwachstellen für die Schwachstellenscanner des BSI
- §§ 16,17: Aufhebung der Einschränkungen auf **konkrete** erhebliche Gefahren für die Anordnung von Maßnahmen ggü. Anbietern von Telekommunikationsdiensten
- § 43 (5): **Wegfall** von jährlichen statistischen Meldevorschriften der Geheimdienste für unterdrückte Informationsweitergabe an das BSI
- § 44 (2): **Verpflichtung** des BSI bei Aktualisierungen des IT-Grundschutz und Mindeststandards vor allem die Umsetzungskosten zu minimieren
  Anmerkung: Die Vorabfassung weist hier fälschlicher Weise den „§ 4“ statt den „§ 44“ aus.
- § 58 (1-3): Berücksichtigung der **Zivilgesellschaft** vor dem Erlassen von Rechtsverordnungen **fällt komplett weg**

Details zu diesen Punkten sind in den weiteren Erläuterungen eingearbeitet.

Die **bisherigen aufgeführten Defizite** bleiben weiterhin bestehen und sind somit weiterhin gültige Forderungen der AG KRITIS.

Definition Kritischer Infrastrukturen

Bisher definiert § 2 (10) BSI-Gesetz die "Kritische Infrastrukturen". Mit der Umsetzung der NIS2-Richtlinie wird dies nunmehr ersetzt durch eine Unterscheidung in "Besonders wichtige Einrichtungen" (BWE) und "wichtige Einrichtungen" (WE) sowie als Teil der BWE die "Betreiber kritischer Anlagen". Die Definitionen als BWE oder WE sind einerseits an Schwellwerte der Beschäftigten und des Umsatzes gebunden (sogenannte EU-Size Cap Regelung), und andererseits an eine klare Sektorendefinition in den Anlagen 1 und 2 des NIS2UmsuCG. Für "kritische Anlagen", welche den bisherigen KRITIS-Anlagen entsprechen, gilt weiterhin eine noch zu erlassende Rechtsverordnung, welche dann die bisherige Kritisverordnung ersetzen soll.

Klar ist damit, dass die Regelungen über Kritische Infrastrukturen (KRITIS) deutlich komplexer einerseits und umfassender andererseits werden. Während wir als AG KRITIS eine umfassendere Auslegung der KRITIS begrüßen, sehen wir erhöhte Komplexität KRITISch:

Einrichtungen sollten idealerweise an einheitlich definierten Sektoren und weiteren Kennzahlen (Umsatz, versorgte Bevölkerung, regionales Versorgungsmonopol uvm.) klar und rechtlich eindeutig identifizieren können, ob sie als KRITIS gelten. Insbesondere unterschiedliche Definitionen der Sektoren in den unterschiedlichen Kategorien (Besonders wichtige Einrichtungen, wichtige Einrichtungen, kritische Anlagen) und Anlagen erhöhen hier die Komplexität bereits in der Betroffenheitsprüfung drastisch, Stichwort Bürokratie.

Definitionen wie "kritische Anlagen" können § 56 entsprechend durch Rechtsverordnungen konkretisiert werden. Diese werden durch das BMI im Zusammenwirken mit anderen Ministerien erarbeitet. Bereits im Entwurf vom 07.05.2024 wurde in Absatz 4 die **Einbindung der Zivilgesellschaft** für die Definition von „kritischen Anlagen“ **entfernt**. Im aktuellen Referentenentwurf wurde diese **fehlgeleitete Anpassung** auf alle 5 Absätze des Artikels **ausgeweitet** und betrifft somit die Definition von kritischen Anlagen, erheblichen Sicherheitsvorfällen, die Verfahren zur Erteilung von Sicherheitszertifikaten, wann die Sicherheitszertifikate verpflichtend sind, sowie das Sicherheitskennzeichen. Entgegen der bisherigen Praxis als auch dem Koalitionsvertrag sollen Akteure aus der Wirtschaft und der Wissenschaft nicht (mehr) eingebunden werden.

Für alle Regelungen des § 56 fordern wir weiterhin die verbindliche Einbindung der Zivilgesellschaft, die bisher und offenbar auch zukünftig weiterhin keine Berücksichtigung finden soll.

Aufgrund der Komplexität der Regelungen fallen weitere Sonderfälle auf, wie hier am Beispiel des Sektors Forschung aufgezeigt wird: so wird der Sektor Forschung gemäß der Begriffsdefinition "Forschungseinrichtung" auf angewandte Forschung mit kommerziellem Zweck begrenzt. Nach Ansicht der AG KRITIS ist hier auch die Grundlagenforschung als Kritische Infrastruktur zu betrachten. Insbesondere, wenn diese sicherheitsrelevante Auswirkungen haben kann.

Auf der Webseite „EduSec: Sicherheitsvorfälle an deutschsprachigen Hochschulen“ unter www.aheil.de/edusec/ können alle öffentlich bekannt gewordenen Vorfälle eingesehen werden, die ehrenamtlich dort gesammelt und veröffentlicht werden.

Durch den Bund finanzierte Forschungseinrichtungen, welche in der Rechtsform einer Stiftung des öffentlichen Rechts nach Landesrecht aufgebaut wurden, sind darüber hinaus ebenfalls nicht von den Regelungen des Gesetzes erfasst, außer es wird ihnen im Einvernehmen mit dem zuständigen Ressort angeordnet.

Generell werden Bundesbehörden, öffentlich-rechtlich organisierte IT-Dienstleister der Bundesverwaltung sowie weitere Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts sowie ihre Vereinigungen, ungeachtet ihrer Rechtsform lediglich als Einrichtungen der Bundesverwaltung im Sinne des Gesetzes angesehen, sofern dies durch das BSI im Einvernehmen mit dem jeweils zuständigen Ressort angeordnet wurde.

Auch hier braucht es verbindliche Anforderungen zur Umsetzung von Cybersicherheitsmaßnahmen, da die Selbstregulierung auch in diesen Fällen nicht greift.

KRITIS Sektor Staat und Verwaltung

Für den KRITIS Sektor Staat und Verwaltung gelten im Zuge des NIS2UmsuCG **unzählige Sonderregelungen und Ausnahmen**. Damit unterliegt die Verwaltung insbesondere des Bundes wieder zahlreichen Sonderregelungen und die Verwaltungen auf Kommunaler und Bundeslandebene werden vollständig außen vor gelassen und überhaupt nicht adressiert. Dies ist im Hinblick auf die vielen und teilweise sehr weitreichenden Cybersicherheitsvorfälle wie Landkreis Anhalt Bitterfeld oder SIT.NRW (über 100 Kommunen waren monatelang betroffen und faktisch handlungsunfähig!) nicht mehr nachvollziehbar. Offensichtlich soll der Jahrzehnte gepflegte Investitionsstau weiterhin aufrecht gehalten werden. Die Kette an Cybersicherheitsversagen und Verantwortungsdiffusion kann beispielsweise unter einer ehrenamtlich gepflegten Webseite[3] eingesehen werden und erweitert sich derweil kontinuierlich. Dies zeugt nicht von ernstgemeintem Verständnis, was nach § 2 Nr. 24:

> *„kritische Dienstleistung“ eine Dienstleistung zur Versorgung der Allgemeinheit in den Sektoren Energie, Transport und Verkehr, Finanzwesen, Sozialversicherungsträger sowie Grundsicherung für Arbeitssuchende, Gesundheitswesen, Wasser, Ernährung, Informationstechnik und Telekommunikation, Weltraum oder Siedlungsabfallentsorgung, deren Ausfall oder Beeinträchtigung zu erheblichen Versorgungsengpässen oder zu Gefährdungen der öffentlichen Sicherheit führen würde;*

ist bzw. es soll dieses Jahrzehnte gepflegte systemische Versagen weiterhin aufrecht erhalten bleiben, was in keinster Weise nachvollziehbar ist.

Kommunale Selbstverwaltung und Föderalismus sind ein hohes Gut, was nur dadurch aufrecht gehalten werden kann, wenn die Kommunen und Landkreise eine entsprechende Cybersicherheitsstärkung erhalten, da sie eigenständig dazu nicht in der Lage sind. Dies nicht zu berücksichtigen, ist für die AG KRITIS äußerst fahrlässig, da die betroffene Bevölkerung keine Handlungsalternative hat und die Kommunen und Landkreise eigenständig schlicht keine angemessenen Ressourcen einbringen können.

Es ist zwar nachvollziehbar, dass der Bundesgesetzgeber aus kompetenzrechtlichen Gründen derzeit nicht selbst tätig werden kann. **Es ist aber dann umso wichtiger, dass sowohl die Vertreter der Bundesregierung als auch die Mitglieder des Bundestages die Notwendigkeit entsprechender IT-Sicherheitsregelungen für Länder und Kommunen bei ihren jeweiligen Pendants auf Ebene der Länder adressieren.**

Denn im föderalen Staat sind sie es, die die Pflicht zur Umsetzung europäischer Richtlinien trifft, wo das Grundgesetz ihnen die Gesetzgebungs- und Verwaltungskompetenz zuweist. Leider muss derzeit jedoch konstatiert werden, dass diese Verpflichtung auf Länderebene teilweise nicht wahrgenommen wird.

So sehr zu begrüßen ist, dass der Sektor Staat und Verwaltung damit erstmals umfassend nach KRITIS-Gesichtspunkten reguliert wird, so sehr sehen wir auch, dass hier die Chance auf eine einheitliche Regelung für alle Ebenen des Sektors Staat und Verwaltung vertan wird.

Dies sieht der Bundesrechnungshof in seinem *„Bericht nach § 88 Absatz 2 BHO an den Haushaltsausschuss des Deutschen Bundestages und den Ausschuss für Inneres und Heimat des Deutschen Bundestages zum Regierungsentwurf des NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetzes (NIS2UmsuCG)“* vom 17.09.2024 identisch: *„Die Bundesregierung läuft Gefahr, ihr Ziel zu verfehlen, die Informations- und Cybersicherheit zu verbessern. Sie will die NIS-2-Richtlinie der Europäischen Union 1:1 umsetzen, ihr bereits*

[3] https://kommunaler-notbetrieb.de

bekannte Defizite dabei jedoch nicht aufgreifen. Wenige Änderungen am Gesetzentwurf könnten das Sicherheitsniveau in der Bundesverwaltung deutlich erhöhen.“

Das NIS2UmsuCG setzt offenbar nur die durch die EU erzwungenen Cybersicherheitsmaßnahmen für Deutschland minimalistisch (1:1 Umsetzung) um und vermeidet jedwede weitere Möglichkeit der Cyberresilienz oder Cybersicherheitsstärkung.

Zuvorderst begrüßt die AG KRITIS die Einführung des "CISO Bund" (Koordinatorin oder Koordinator für Informationssicherheit). Jedoch sind wir verwundert, dass in § 48 keine Aussagen darüber getroffen werden, wo genau diese Rolle eingerichtet werden soll: hier fordern wir insbesondere eine Unabhängigkeit des „CISO Bund“ vom "CIO Bund" und auch dem Bundesamt für Sicherheit in der Informationstechnik (BSI), um so eine wirkungsvolle Kontrollinstanz darstellen zu können. Idealer Weise ist er auch vom Bundesministerium des Innern und für Heimat (BMI) unabhängig und beispielsweise im Bundeskanzleramt als Stabsstelle zu verankern.

Darüber hinaus wurde dieses Amt weder mit angemessenen Aufgaben, noch mit angemessenen Befugnisse ausgestattet.

Für Einrichtungen der Bundesverwaltung finden nach § 29 (2) im NIS2UmsuCG grundsätzlich die Regelungen für "besonders wichtige Einrichtungen" Anwendung, wobei hiervon teilweise unverständlicher Weise die folgenden Regelungen ausgenommen werden sollen:

- § 30 - Keine Risikomanagementmaßnahmen (lediglich für Bundeskanzleramt und die Bundesministerien)
- § 38 - keine Haftungsregelungen für Geschäftsleitungen
- § 40 (3) - Keine Zusammenarbeit mit dem BSI für beispielsweise Lagebilder
- § 61 - Aufsichts- und Durchsetzungsmaßnahmen
- § 65 - Keine Bußgeldvorschriften

Der Ausschluss des § 30 adressiert den Kern der Cybersicherheitsmaßnahmen. Maßnahmen nach Stand der Technik wie z.B. Risikoanalysen, Bewältigung von Sicherheitsvorfällen, Sicherheit der Lieferkette, Management und Offenlegung von Schwachstellen, Kryptografie und Verschlüsselung, Sicherheit des Personals und Verwendung von Multi-Faktor-Authentifizierung sind daher allesamt für Einrichtungen der Bundesverwaltung nicht ausschlaggebend und nicht zu berücksichtigen, sofern diese nicht in Mindeststandards des BSI geregelt sind. Offenbar können Einrichtungen der Bundesverwaltung Cybersicherheit Kraft Magie realisieren. Dieser Ausschluss erzeugt starkes Kopfschütteln und lässt uns mit Verwunderung und Fassungslosigkeit zurück.

§ 29 (2) sollte daher wie folgt angepasst werden:

„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.**~~“

Mit dem Ausschluss des § 38 werden "Geschäftsleitungen" der Bundesverwaltung von den mit der NIS2-Regulierung eingeführten Billigungs-, Überwachungs- und Schulungspflicht von Ihrer Verantwortung befreit. Zwar weist ihnen § 43 dann entsprechende Pflichten zu, ohne jedoch auch eine dem § 38 (2) entsprechende

Haftungsregelung vorzusehen. Das ist für die AG KRITIS nicht nachvollziehbar. **Denn ohne drohende negative Konsequenzen ist der Handlungsdruck bei den agierenden Personen begrenzt.**

Auch der Ausschluss der Bundesverwaltung von § 40 (3) ist hierbei nicht nachvollziehbar. Die Regelung in sich wirkt nicht konsistent, da insbesondere hier ja zu Lagebildern und Erkenntnisgewinn beigetragen werden kann. Dies speziell im Hinblick auf Desinformationskampagnen, Trollfabriken, Kriminellen Organisationen, Geheimdiensten und anderen staatlichen Akteuren in Regierungsnetzen und dem **von Vorfällen bereits betroffenen Auswärtigen Amt oder sogar in Bundeskanzlerin Merkels Rechner** (zu dem es sogar einen Podcast[4] investigativer Recherche gab).

Es fällt auf, dass in dem vorliegenden Gesetzesentwurf die Durchsetzungsbefugnisse aus § 61 nicht gegenüber den Stellen des Bundes gelten sollen. Zwar werden etwa in Bezug auf Kontrollen und Prüfungen ähnliche Regelungen in § 7 eingeführt. Diese ermöglichen dem BSI auch, Audits und Prüfungen durchzuführen und daraus Maßnahmen und Anweisungen abzuleiten. Sowohl in Bezug auf die Stellen des Bundes als auch auf die übrigen wichtigen und besonders wichtigen Einrichtungen wird die Wirksamkeit der Regelungen aber von der tatsächlichen Prüf- bzw. Kontrolldichte abhängen. Bereits jetzt ist absehbar, dass das BSI nicht ausreichend Ressourcen für alle Aufsichtsaufgaben erhalten wird. Daher sollte im Gesetz zumindest klargestellt werden, dass regelmäßige Kontrollen der genannten Einrichtungen nicht nur zu den Befugnissen des BSI gehören, sondern zu den Pflichtaufgaben.

Es sollte daher ein neuer § 3 (4) ergänzt werden:

„Das Bundesamt prüft regelmäßig, ob wichtige und besonders wichtige Einrichtungen sowie Einrichtungen der Bundesverwaltung, die notwendigen Vorkehrungen zur Absicherung ihrer informationstechnischen Systeme, Komponenten und Prozesse ergriffen haben, um den Pflichten aus diesem Gesetz gerecht zu werden."

Um **sowohl gegenüber der Bevölkerung als auch gegenüber dem Parlament Klarheit** darüber zu verschaffen, wie das BSI seine dahingehende Kontrollaufgabe wahrnimmt, sollte es beide **regelmäßig darüber unterrichten**. Eine entsprechende Verpflichtung sollte in § 58 (2) ergänzt werden:

„Die Unterrichtung umfasst insbesondere die Zahl der Fälle, in denen das Bundesamt von seinen Prüf- und Kontrollbefugnissen nach § 7 und § 61 dieses Gesetzes Gebrauch gemacht hat."

Weiterhin werden mit § 29 (1) Nr. 2 im weitesten Sinne alle öffentlichen IT-Dienstleister (Cloud-Computing-Diensten, Anbieter von Rechenzentrumsdiensten, Vertrauensdiensteanbieter, Managed Service Provider und Managed Security Services Provider) ausgeschlossen, welche Dienste für Landes- oder Kommunalverwaltungen anbieten und bereits durch die Länder (wie auch immer geartet) reguliert wurden.

Die AG KRITIS fordert auch hier wieder eine klare, bundeseinheitliche Regelung für öffentliche IT-Dienstleister auf allen Ebenen – der Bundesebene, der Bundeslandebene und der Kommunalen Ebene, denn Cyberangriffe und Datenpakete machen keine Ebenenunterscheidung im Cyberraum. **Die AG KRITIS sieht - so wie auch das Grundgesetz - den Bund in der Pflicht, einheitliche Lebens- und Sicherheitsstandards für öffentliche Dienstleistungen der Daseinsvorsorge zu gewährleisten.** Dies kann nur ohne Benachteiligung erfolgen, wenn diese länderübergreifend einheitlich definiert sind. Gerade die IT-Sicherheitsvorfälle der vergangenen Monate und Jahre und die hohe Zahl an öffentlichen IT-Dienstleistern, die mehrere Kommunen und Länder bedienen, zeigt die Kritikalität dieser Dienste für die Öffentlichkeit und für alle Bürgerinnen. Eine Unterscheidung nach

[4] https://www.br.de/mediathek/podcast/der-mann-in-merkels-rechner-jagd-auf-putins-hacker/853

Zuständigkeiten, Ebenen oder Schwellenwerten würde Bürgerinnen aus Sicht der AG KRITIS in unterschiedliche Versorgungsklassen einordnen, was in deutlichem Widerspruch zu Gleichheitsgebot und Daseinsvorsorge steht.

Sofern darüber hinaus die Einrichtungen der Bundesverwaltung in § 43 (4) Satz 2 erst nach fünf(!) Jahren erstmalig und danach nur „regelmäßig“ statt beispielsweise „anschließend alle drei Jahre“ dem BSI die Erfüllung der Anforderungen nachweisen sollen, wird die überaus lückenhafte Umsetzungsanforderung noch unnötig sehr stark verzögert.

Ausnahmen als Regelfall

In § 37 Ausnahmebescheid wird ein Großteil der Funktionsfähigkeit eines souveränen Staates ausgeklammert. **Das BMI, das Bundeskanzleramt, das BMJ, das BMV, das BMF und die Innenministerien der Bundesländer können BWE oder WE ganz oder teilweise von diesem Gesetz ausnehmen.**

Auch **alle Einrichtungen, die in den Bereichen nationale Sicherheit, öffentliche Sicherheit, Verteidigung oder Strafverfolgung, einschließlich der Verhütung, Ermittlung, Aufdeckung und Verfolgung von Straftaten, (relevante Bereiche) tätig sind oder Dienste erbringen** können dadurch von den Risikomanagementmaßnahmen nach § 30 und den Meldepflichten nach § 32 befreit werden.

Auch **alle Einrichtungen, die ausschließlich für Behörden, die Aufgaben in relevanten Bereichen erfüllen, tätig sind oder Dienste erbringen**, können von den Risikomanagementmaßnahmen nach § 30 und den Meldepflichten nach § 32 befreit werden.

Ein funktionaler und souveräner Staat macht sich bei Bürgerinnen in erster Linie im Rathaus und funktionierenden Fachverfahren in den Landkreisen und Kommunen aus. In zweiter Linie in der (demokratischen) Funktionsfähigkeit der o.g. Strafverfolgungsbehörden und weitern BOS etc. Falls diese weiterhin von den Cybersicherheitsanforderungen ausgenommen werden und dadurch weggecybert werden, wird die **Destabilisierung der Bevölkerung von innen** weiter voranschreiten und nicht aufzuhalten sein.

Risikomanagement, Haftung der Geschäftsleitung und Durchsetzungsmaßnahmen

Mit § 30 des NIS2UmsuCG werden umfassende Maßnahmen zum Risikomanagement für BWE und WE eingeführt, welche nach § 31 für Betreiber kritischer Anlagen zusätzlich verschärft werden. Diesen umfassenden Maßnahmenkatalog begrüßen wir ausdrücklich und bedanken uns vorab beim Gesetzgeber für den Willen zur Umsetzung bereits im Jahre ~~**2024**~~ **2025**.

Vor allem stellen wir fest, dass die hiermit definierten Maßnahmen die reine Cybersicherheitsbetrachtung zur Umsetzung eines Informationssicherheits-Managementsystems (ISMS) überschreiten. Insbesondere die Rollen des Business Continuity Management (BCM) und des IT Service Continuity Management (ITSCM) werden hiermit in den betroffenen Einrichtungen gefordert und gestärkt, sowie zusätzlich zentrale Kapazitäten im organisationsweiten Krisenmanagement gefordert. Wir sehen dies als notwendige Voraussetzungen dafür, um Kritische Infrastrukturen als auch BWE und WE umfassend vor Gefahren zu schützen, welche die Geschäftstätigkeit gefährden, sowie die Fortführung der kritischen Dienstleistungen auch bei Sicherheitsvorfällen zu gewährleisten. Die Vergangenheit hat gezeigt, dass Einrichtungen in der Selbstregulierung schlicht versagt haben und die bestehenden Anforderungen an KRITIS-Betreiber nicht ausreichen, um die Versorgungssicherheit der Bevölkerung zu gewährleisten.

Der Bitkom Verband mit über 2.200 Mitgliedsunternehmen stellt dazu in einer aktuellen Veröffentlichung[5] fest:

„8 von 10 Unternehmen von Datendiebstahl, Spionage oder Sabotage betroffen. Rekordschaden von rund 267 Milliarden Euro."

Offensichtlich belegen diese Zahlen, dass die deutsche Wirtschaft nicht in ihrer Selbstverantwortung Willens ist, die Versorgungssicherheit der Bevölkerung zu gewährleisten.

Sowohl in der Definition eines Sicherheitsvorfalls nach § 2 Nr. 40, als auch bei der Definition von Risikomanagementmaßnahmen nach § 30 (1) wurde die Authentizität als Schutzziel entfernt. Ebenso wurde sie in den Schutzzielen des § 2 Nr. 23 für kritische Komponenten / IKT-Produkte gestrichen. Dies unterscheidet sich von vorherigen Entwürfen des NIS2UmsuCG, sowie auch von den aktuellen Anforderungen des § 8a BSI-Gesetz. Auch wenn das Sicherstellen der Authentizität mit den unter § 30 (1) festgelegten Maßnahmen angestrebt werden soll, ist deren Verletzung demnach zukünftig nicht mehr als Sicherheitsvorfall zu bewerten. Die Klarstellung in der Begründung Teil B zu § 2 Nr. 1, die in der NIS-2 erwähnte Authentizität sei im deutschen Recht ein Unterfall der Integrität, adressiert die fachlich richtige und relevante Unterscheidung unzureichend. Eine Verletzung des Schutzziels Authentizität kann selbstverständlich auch zu erheblichen Folgen führen, sowohl bei der IT-basierten Kommunikation von Menschen untereinander, aber insbesondere auch bei der technischen Kommunikation von Kritischen Infrastrukturen. Daher sehen wir es als gegeben an, dieses Schutzziel weiterhin explizit aufzuführen.

Sowohl für BWE als auch für WE sollen in §§ 61-62 umfassende Befugnisse des BSI für Maßnahmen zur Aufsicht und Durchsetzung etabliert werden. Insbesondere die Möglichkeit, sich die Umsetzung von Maßnahmen durch Betreiber kritischer Anlagen, aller anderen BWE sowie der WE nachweisen zu lassen, sowie diese auch extern auditieren zu dürfen, begrüßt die AG KRITIS ausdrücklich.

Insgesamt ergibt sich hieraus erstmals ein begrüßenswertes und umfassendes Set aus Regelungen, Kontroll- sowie Sanktionsmechanismen, auch wenn die Ausnahmeregelungen leider äußerst umfassend ausgereizt werden. Die mit dem § 63 (3) eingeführte Frist von drei Jahren nach Einführung des Gesetzes, insbesondere für BWE, betrachten wir als nicht erforderlich: die EU NIS2-Richtlinie ist seit 2022 verabschiedet und bereits bekannt.

Systeme zur Angriffserkennung

Bedauerlich ist, dass § 58 (2) wie die Vorgängerregelung im derzeit geltenden BSIG § 8a weiterhin eine Pflicht für den Einsatz von Systemen zur Angriffserkennung vorsieht. Dagegen hatte sich die AG KRITIS bereits im Rahmen der Ausschussanhörung zum zweiten IT-Sicherheitsgesetz ausgesprochen[6].

Es ist **aus Sicht des Risikomanagements als auch aus technischer Sicht unsinnig**, bestimmte Einzelmaßnahmen wie Systeme zur Angriffserkennung explizit im Gesetz zu nennen. Denn welche konkreten Maßnahmen zur Absicherung in welcher Risikopriorisierung ergriffen werden müssen, ergibt sich aus einer Risikoanalyse im Rahmen des ISMS mit BCM nach § 30 (Risikomanagementmaßnahmen besonders wichtiger Einrichtungen und wichtiger Einrichtungen).

Wenn den Maßnahmen zur Angriffserkennung durch die explizite Nennung im Gesetzestext entsprechende Priorität einzuräumen ist, fehlen die dafür aufzuwendenden Ressourcen im Zweifel bei den Maßnahmen, die nach

[5] https://www.bitkom.org/Presse/Presseinformation/Wirtschaftsschutz-2024
[6] https://ag.kritis.info/2021/03/01/stellungnahme-zum-it-sicherheitsgesetz-2-0-im-innenausschuss-des-bundestags/

der Risikoanalyse in der Priorität wichtiger und dringend nötiger sind, z.B. eine angemessen abgesicherte Fernwartung nach dem Stand der Technik.

Bei dem durch die EU an Russland attribuierten Angriff[7] gegen das Viasat Satellitennetzwerk KA-SAT beispielweise „a ground-based network intrusion by an attacker exploiting a misconfiguration in a VPN appliance to gain remote access to the trusted management segment of the KA-SAT network“[8] oder wie sie im Fall eines Wasserwerks in Texas[9] ebenfalls unzureichend vorhanden war.

Auch in Deutschland sind aktuell solche Szenarien im Betrieb via Fernwartung weiterhin Alltag. Dort wo sie nach einer Risikoanalyse als notwendige Maßnahme identifiziert werden, zählen Angriffserkennungssysteme auch schon seit dem IT-Sicherheitsgesetz von 2015 zu den technischen Maßnahmen, die nach § 8a (1) BSIG umzusetzen waren. In der Gesetzesbegründung zum IT-Sicherheitsgesetz 2015 werden solche Detektionsmaßnahmen explizit als Teil der Absicherungspflichten nach § 8a (1) BSIG genannt[10]. Um eine wirklich risikoadäquate Absicherung zu ermöglichen, sollte die Verpflichtung auf die Einzelmaßnahme der Angriffserkennungssysteme in § 31(2) gestrichen werden.

Mangelhafte Unabhängigkeit des BSI

Das BSI wird weiterhin - im Widerspruch zum Ampel-Koalitionsvertrag, nach dem die Unabhängigkeit erweitert werden sollte - fachlich und dienstlich vom BMI unverändert beaufsichtigt, da der § 1 weiterhin so und unverändert bestehen bleibt. Wenn das BSI als solches weiterhin leider nicht unabhängig zum BMI werden soll, bedarf es einer vom BMI unabhängigen Kontrolle der umfassenden Tätigkeiten und Rechtsbefugnisse des BSI, die über die Berichtspflichten des BSI gemäß § 58 an das BMI hinaus gehen.

Technische Expertise und Befugnisse des BSI

Das BSI hat über Jahre hinweg die beachteten IT-Grundschutz- und Mindeststandards nach dem Stand der Technik entwickelt und dafür Anerkennung bekommen. Es ist unverständlich, warum dieser Sachverstand in § 44 (2) mit dem Zusatz „dabei wird der Umsetzungsaufwand soweit möglich minimiert“ mit einem Dämpfer versehen wird, um billige Maßnahmen durchzusetzen. Die Bewertung nach Stand der Technik hat bereits die Angemessenheit der empfohlenen Maßnahmen berücksichtigt.

Darüber hinaus empfiehlt die AG KRITIS dringend, § 44 (1) Satz 1 wie folgt anzupassen, um Cybersicherheit in der Bundesverwaltung aufrichtig und dauerhaft zu etablieren:

„Die Einrichtungen der Bundesverwaltung müssen die ~~**jeweils geltenden Fassungen der**~~ Mindeststandards für die Sicherheit in der Informationstechnik des Bundes (Mindeststandards)**, die BSI-Standards und das IT-Grundschutz-Kompendium des Bundesamtes (IT-Grundschutz) in den jeweils geltenden Fassungen** als Mindestanforderungen zum Schutz der in der Bundesverwaltung verarbeiteten Informationen erfüllen.“

[7] https://www.consilium.europa.eu/de/press/press-releases/2022/05/10/russian-cyber-operations-against-ukraine-declaration-by-the-high-representative-on-behalf-of-the-european-union/
[8] https://news.viasat.com/blog/corporate/ka-sat-network-cyber-attack-overview
[9] https://www.lebensraumwasser.com/hackerangriff-auf-wasserwerk-in-den-usa/
[10] BT-Drucksache 18/4096, Seite 25.

§ 44 (2) Satz 1 und 2 sind des Weiteren wie folgt anzupassen:

„~~**Das Bundeskanzleramt und die Bundesministerien müssen als zusätzliche Mindestanforderungen dD**~~ie BSI-Standards und das IT-Grundschutz-Kompendium des Bundesamtes (IT-Grundschutz) werden in den jeweils geltenden Fassungen ~~**einhalten. Die jeweils geltenden Fassungen werden**~~ auf der Internetseite des Bundesamtes veröffentlicht.“

Weiterhin hat das BSI die letzten Jahre durch regelmäßige Schwachstellenscans und dem direkten Kontaktieren von Betreibern verwundbarer Systeme konkret zur Cybersicherheit im Land beigetragen. Die Einschränkungen auf lediglich „bekannte“ Schwachstellen in § 15 (1) ist nicht nachvollziehbar, da hiermit dem BSI weitere defensive aber hilfreiche technische Möglichkeiten versagt werden.

Zur Abwehr von laufenden Angriffskampagnen (konkrete erhebliche Gefahr) gegen Kommunikationstechnik des Bundes, BWE, WE, Telekommunikationsdienste oder eine erhebliche Anzahl von Systemen, kann das BSI technische Maßnahmen gegenüber Anbietern von Telekommunikationsdiensten (§ 16) und von digitalen Diensten (§ 17) anordnen. Wir begrüßen, dass der zwischenzeitlich gestrichene Begriff „konkret“ wieder ergänzt wurde, denn sonst würden dadurch massive Eingriffe in Systeme wie „technische Befehle zur Bereinigung“ bei einer wesentlich niedrigeren Schwelle möglich, was bei Fehlen eines Angriffs und somit von Gefahr im Verzug nicht nachvollziehbar ist.

Meldepflicht

Die AG KRITIS begrüßt die in § 32 definierte gemeinsame Meldestelle für das BSI sowie das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK). Insbesondere im Hinblick auf das parallel in der Umsetzung befindliche KRITIS-Dachgesetz, da physische Sicherheit und Cybersicherheit als auch das dafür zu betreibende Krisenmanagement Hand in Hand agieren muss. Sicherheitsvorfälle jedweder Art sollten daher zentral und einheitlich an eine Meldestelle kommuniziert werden. Die AG KRITIS empfiehlt daher auch, dies beispielsweise bei derzeit darüber hinaus gehenden Meldungen an die Bundesnetzagentur (BNetzA) und die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) so zu vereinheitlichen. Bürokratie und Komplexität sind der Feind der Sicherheit, auch bei der Meldung von Sicherheitsvorfällen.

In § 43 (5) werden Einrichtungen der Bundesverwaltung darüber hinaus aufgefordert „alle für die Abwehr von Gefahren für die Sicherheit in der Informationstechnik erforderlichen Informationen, insbesondere zu Schwachstellen“ unverzüglich zu melden. Dies konnte aber zum Beispiel aufgrund von Regelungen zum Geheimschutz oder Vereinbarungen mit Dritten (ja, ein NDA reicht) unterbleiben. Es muss aber zum Jahresende eine Statistik über die so unterdrückten Meldungen an das BSI übermittelt werden. Die AG KRITIS bedauert, dass selbst diese statistische Auswertung für den Bundesnachrichtendienst und das Bundesamt für Verfassungsschutz ausbleiben soll. **Dadurch wird auch den Kontrollgremien wichtige Transparenz über die Verheimlichung von dem Staat bekannten Schwachstellen genommen.**

Empfehlungen des Bundesrechnungshofes

Die AG KRITIS schließt sich den Empfehlungen des Bundesrechnungshofes in seinem „Bericht nach § 88 Absatz 2 BHO an den Haushaltsausschuss des Deutschen Bundestages und den Ausschuss für Inneres und Heimat des Deutschen Bundestages zum Regierungsentwurf des NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetzes (NIS2UmsuCG)“ vom 17.09.2024 vollständig an. Die darin aufgeführten **Empfehlungen sollten dringend allesamt realisiert werden**!

Schwachstellenmanagement

Im Rahmen der *AG BSI* hat unser Gründer und Sprecher Manuel ‚HonkHase' Atug bereits dargelegt, dass Schwachstellen nicht verwaltet, sondern geschlossen werden müssen.

Das Gesetz sollte daher klarstellen, dass dem BSI gemeldete Informationen ausschließlich für den Schutz der IT-Sicherheit verwendet werden dürfen und der **Einsatz oder die Verwendung von Schwachstellen für offensive oder invasive Zwecke nicht zulässig** ist. Um ein hohes Maß an IT-Sicherheit erreichen zu können, sind alle Sicherheitsbehörden wie z. B. BND, BKA, Bundespolizei, Verfassungsschutz, ZITiS und die Bundeswehr zu verpflichten, von ihnen gefundene oder erworbene Schwachstellen ausnahmslos an das BSI zu melden.

Es braucht diese ausnahmslose Meldepflicht entdeckter Sicherheitslücken, die für alle staatlichen Stellen gelten muss. Ohne ein solch klares Bekenntnis des Gesetzgebers - auch zur Rolle des BSI hin - droht ansonsten ein schwerwiegender Vertrauensverlust bei den relevanten Akteuren aus der Wissenschaft, Wirtschaft, Zivilgesellschaft und den Sicherheitsforscherende.

Zum Thema „Zurückhalten von Schwachstellen" hatte sich die AG KRITIS bereits im Rahmen der Ausschussanhörung zum zweiten IT-Sicherheitsgesetz hinreichend ausgesprochen[11].

Würdigung des Prozesses

Abschließend betonen wir als AG KRITIS erneut, dass ein transparenter Prozess in der Gesetzgebung sowie umfassende und zeitlich angemessene Beteiligungsverfahren der Wirtschaft, Wissenschaft und Zivilgesellschaft bei derart tiefgreifenden und weitreichenden Gesetzgebungsverfahren dringend geboten ist.

Insbesondere hinsichtlich einer einheitlichen und kongruenten Regulierung im KRITIS-Umfeld betrachten wir als AG KRITIS eine gleichzeitige Veröffentlichung und Diskussion von Gesetzesentwürfen zur Umsetzung der NIS2-Richtlinie (NIS2UmsuCG) und CER-Richtlinie (KRITIS-Dachgesetz) sowie der im NIS2UmsuCG vorgesehenen Verordnungen für zwingend erforderlich.

Fazit

Es scheint, als sei weiterhin keine vollständige Harmonisierung der Regelungen zwischen den beiden Gesetzesvorlagen erfolgt - was aktuell aufgrund der mangelnden Transparenz nicht überprüfbar ist. **Übrig bleibt eine unsichere Lage bei allen potenziell betroffenen Einrichtungen und ihren Lieferketten, sowie bei allen verantwortlichen Aufsichtsbehörden und Zuständigen für die Umsetzung und Einhaltung** der kommenden Regulierungen als auch bei der Wissenschaft, Forschung und zuletzt auch der fachkundigen Bevölkerung, die willens sind, ihren Beitrag durch Fachexpertise ehrenamtlich und kostenfrei beizutragen, dies aber nicht angemessen in den intransparenten Dialog einbringen können.

[11] https://ag.kritis.info/2021/03/01/stellungnahme-zum-it-sicherheitsgesetz-2-0-im-innenausschuss-des-bundestags/

Abgeordnete haben im Rahmen der 1. Lesung zum NIS2UmsuCG im Bundestag auf Cyberdurchfall hingewiesen.

Der Bundesrechnungshof stellt fest: „Wichtige Regelungen sollen nicht für die gesamte Bundesverwaltung in einheitlicher Weise verbindlich sein. Die Folge wäre ein **„Flickenteppich“**, der die Informations- und Cybersicherheit aller Beteiligten gefährden kann.“

Manuel ‚HonkHase‘ Atug, Gründer und Sprecher der unabhängigen AG KRITIS sagt dazu: „Wir brauchen dringend eine **strikt defensive Cybersicherheitsstrategie**, statt dem immer wieder vorgelegten und großflächig zerfaserten Cyberdiarrhö an Lücken, Ausnahmen und offensiven Optionen. Eine Cybernation Deutschland darüber hinaus kann nur umgesetzt werden, wenn das Cyber-Wimmelbild der Verantwortungsdiffusion bereinigt und konsolidiert wird“.