21. Wahlperiode

Deutscher Bundestag
Innenausschuss

Ausschussdrucksache 21(4)062 E
vom 13. Oktober 2025

Schriftliche Stellungnahme

von Sabine Griebsch, Management Director bei GovThings vom 12. Oktober 2025

Öffentliche Anhörung

Gesetzentwurf der Bundesregierung

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

BT-Drucksache 21/1501

Schriftliche Stellungnahme zur öffentlichen Anhörung zum Gesetzentwurf der Bundesregierung „Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung“ (BT-Drucksache 21/1501)

Allgemeine Vorbemerkung zur Person

- **Cyber- und IT-Krisenmanagerin**, mit Schwerpunkt kommunale Verwaltungen

- Tätigkeiten für die Landkreisverwaltung Anhalt-Bitterfeld als **externe Chief Digital Officer** des Landkreises Anhalt-Bitterfeld sowie als **technische Einsatzleiterin** im Katastrophenschutzstab der Landkreisverwaltung im Zuge der Reaktion und Bewältigung der Folgen des Ransomware-Angriffs/Katastrophenfalls und weitere Einsätze als **IT-Krisenmanagerin** in weiteren Kommunen

- Tätigkeit im Ministerium des Innern des Landes Sachsen-Anhalt und für verschiedene Landesverbände in den Themenbereichen **Föderales Informationsmanagement (FIM), D115, Geodaten und Geodateninfrastruktur, Open Data** und **Sensordaten**.

- Ehrenamtliche Tätigkeit im **Dialog für Cybersicherheit** des Bundesamtes für Sicherheit in der Informationstechnik
    - **Dialogkomitee**, Stakeholdergruppe „Staat“
    - **Initiatorin und Mitwirkung** im Workstream „Cyberresilience-Framework“

- Gründungsmitglied **Kooperative Resilienz e.V.** – Verein zur Stärkung kooperativer kommunaler **Strukturen / Clearingstelle** Kommunaler IT-Notbetrieb (in Gründung)

„Informationssicherheit ist digitale Daseinsvorsorge“[1]

[1] Ina Scharrenbach, MdL, Ministerin für Digitalisierung des Landes Nordrhein-Westfalen

Die Cybersicherheitslage in Deutschland ist weiterhin äußerst angespannt. Nahezu täglich werden **Ransomware-Angriffe**, massive **Datenabflüsse** und das Ausnutzen **kritischer Sicherheitslücken** öffentlich bekannt. Insbesondere staatliche und kommunale IT-Infrastrukturen stehen zunehmend im Visier von Cyberkriminellen und staatlich gesteuerten Angreifern. So wurden in jüngerer Zeit laut Branchenangaben **27 kommunale Verwaltungen und Betriebe Opfer von Ransomware**, wodurch knapp sechs Millionen Bürgerinnen und Bürger betroffen sind. Die Gefahr eines weitreichenden Zusammenbruchs von Verwaltungsleistungen – mit entsprechenden Folgen für Bürger und Wirtschaft – ist so hoch wie nie zuvor. Dieses hohe Bedrohungsniveau unterstreicht den dringenden Handlungsbedarf.

Vor diesem Hintergrund ist der vorliegende Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (NIS2UmsuCG) ein wichtiger Schritt. Mit der Umsetzung der EU-Richtlinie 2022/2555 (NIS-2) sollen zahlreiche IT-Sicherheitsanforderungen verbindlich festgelegt werden, darunter **Maßnahmen zum Risikomanagement**, Verpflichtungen zu **Schutzvorkehrungen nach dem Stand der Technik** und **Meldepflichten** bei Sicherheitsvorfällen. Zudem werden schärfere Sanktionsmöglichkeiten bei Verstößen geschaffen und die Zusammenarbeit der EU-Mitgliedstaaten in der Abwehr von Cyberangriffen verbessert. Diese Maßnahmen sind grundsätzlich geeignet, das Cybersicherheitsniveau in Deutschland deutlich anzuheben und ein klares Signal an alle verantwortlichen Stellen zu senden. Dabei werden damit - abgesehen von den Meldepflichten - nur die Maßnahmen für eine eng umrissene Zielgruppe festgeschrieben, die grundsätzlich zu empfehlen sind.

Gleichwohl wird der aktuelle Gesetzentwurf der realen Bedrohungslage noch nicht vollumfänglich gerecht. Einige wesentliche Bereiche bleiben unzureichend adressiert oder wurden ausgeklammert. Im Folgenden werden die aus meiner Sicht wichtigsten Punkte dargestellt und Empfehlungen für Nachbesserungen gegeben. Ein besonderer Fokus liegt dabei auf der **Einbeziehung der Kommunen** in den Anwendungsbereich des Gesetzes, da gerade hier eine kritische Lücke im Entwurf besteht.

Hiermit nehme ich zum Referentenentwurf des Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (NIS2UmsuCG) Stellung.

Einbeziehung von Kommunen in den Anwendungsbereich der NIS-2-Richtlinie

Kommunen sind die Schnittstelle zwischen Staat und Bürgern. Sie erbringen zahlreiche kritische Dienstleistungen der Daseinsvorsorge und verarbeiten höchst sensible personenbezogene Daten, beispielsweise aus dem Gesundheits- und Sozialbereich.. Gleichzeitig rücken kommunale IT-Netzwerke verstärkt ins Visier von Bedrohungsakteuren. Im Rahmen hybrider Bedrohungsszenarien nutzen staatliche und kriminelle Angreifer Desinformation, DDoS-Angriffe und direkte Angriffe, um kommunale Strukturen

lahmzulegen. Beispiele hierfür sind der Ransomware-Angriff auf die Landkreisverwaltung Anhalt-Bitterfeld im Jahr 2021 sowie der Angriff auf die Stadt Witten durch die russische Gruppe Vice Society, bei dem große Datenmengen entwendet wurden, die wiederum als Informationsquelle für weitere Angriffe dienen.

Spätestens seit Beginn des russischen Angriffskriegs in der Ukraine agieren kriminelle Hackergruppierungen wie politische Akteure, sodass die Grenzen zwischen Kriminalität und staatlicher Cyber-Offensive verschwimmen. Der Verfassungsschutz Nordrhein-Westfalen hat erst kürzlich vor einem erhöhten Risiko russischer Cyberangriffe auf Kommunen gewarnt. Auch Europol betont in seinen Lagebildern (Internet Organized Crime Threat Assessment - IOCTA) die besondere gesellschaftliche Schadwirkung von Cyberangriffen auf Gemeinwesen und Verwaltung. Unter dem Titel „Steal, trade and repeat“ (Stehlen, damit handeln und wiederholen) stellt Europol dabei ausdrücklich fest, dass die Angriffe aggressiver und konfrontativer werden. Damit macht Europol deutlich, dass nicht mehr nur die Erpressung durch Ransomware, sondern das Erlangen von Daten zum Hauptangriffsziel wird – Daten unserer Bürgerinnen, Bürger und Unternehmen.

Vor diesem Hintergrund ist die **Frage der Einbeziehung der Kommunalverwaltungen** in die NIS-2-Umsetzung von zentraler Bedeutung. Art. 2 Abs. 5 der NIS-2-Richtlinie räumt den Mitgliedstaaten die ausdrückliche Option ein, Verwaltungseinrichtungen auf kommunaler Ebene sowie Bildungseinrichtungen in den Anwendungsbereich aufzunehmen. Diese Aufnahme ist keine Pflicht, aber eine Möglichkeit, von der andere EU-Staaten auch Gebrauch machen. Die Bundesregierung hat jedoch entschieden, Kommunen vorerst nicht in das Bundesgesetz aufzunehmen.

In seinem Beschluss 2023/39 vom 03.11.2023 hat der IT-Planungsrat Bund und Länder sogar gebeten, von der Ausweitung auf lokale Ebene keinen Gebrauch zu machen. Stattdessen soll die Absicherung der Kommunal-IT den Ländern überlassen bleiben, etwa durch eigene Landesgesetze oder freiwillige Unterstützungsangebote. Aus meiner Sicht ist diese **Entscheidung nicht zielführend**, da sie den Staat und seine Verwaltung insgesamt **verwundbar** hält und ein **uneinheitliches Schutzniveau** schafft. Dies macht die kommunale Verwaltung zusätzlich verwundbar und angreifbar.

Argumente gegen eine Bundesregelung und warum sie nicht überzeugen

Zur Begründung dieser Ausklammerung werden meist folgende Punkte angeführt:

Föderale Zuständigkeiten: Viele Aufgaben der Verwaltung und IT fallen in Deutschland in den Verantwortungsbereich der Länder und Kommunen. Daher wird argumentiert, dass Regelungen zur kommunalen IT-Sicherheit sollten besser auf Landesebene erfolgen sollten statt durch bundeseinheitliche Vorgaben. Andernfalls drohten Kompetenzkonflikte oder Doppelregelungen zwischen Bund, Ländern und Kommunen.

Überschneidungen vermeiden: Würden Kommunen ins NIS2-Bundesgesetz fallen, könnte es zu Überschneidungen mit bestehenden Landesregelungen kommen. Der IT-Planungsrat wollte solche Unklarheiten offenbar vermeiden und Zuständigkeiten sauber trennen.

Komplexität und Zeitfaktor: Die Umsetzung von NIS 2 ist anspruchsvoll. Indem man die Kommunen ausnimmt, reduziert man zunächst den Adressatenkreis und verschafft den Ländern Zeit, eigene Lösungen zu erarbeiten oder Unterstützungsstrukturen auszubauen, ohne sofort bundesgesetzlichen Druck auf alle Kommunen auszuüben.

Auf den ersten Blick erscheinen diese Punkte pragmatisch. Allerdings überwiegen die **Nachteile einer Nicht-Einbeziehung der Kommunen deutlich:** Die Entscheidung des IT-Planungsrats ist nicht zielführend, da sie keine Alternative aufzeigt, wie auf anderem Wege für IT-Sicherheit in Kommunen gesorgt werden soll.

Anstatt einer dringend nötigen Vereinheitlichung würde der eingeschlagene Weg die bestehende Fragmentierung der Sicherheitsarchitektur in Deutschland verfestigen. Schon heute variiert das Schutzniveau der kommunalen IT erheblich von Region zu Region, da jedes Land eigene Ansätze verfolgt oder teils gar keine spezifischen Vorgaben macht. Einige Länder bieten ihren Kommunen zwar freiwillige Unterstützungsangebote (z.B. Beratung durch Landes-CERTs, Muster-Rahmenwerke etc.), doch diese Ansätze sind uneinheitlich finanziert und reichen nicht aus, um flächendeckend ein hohes Sicherheitsniveau sicherzustellen.

So wurde etwa der Cybersicherheitskompass – ein Portal, das bundesweit alle Unterstützungsangebote von Bund und Ländern für Kommunen auflistete und beschrieb – mangels weiterer Finanzierung eingestellt, ohne dass ein Ersatz geschaffen wurde. Recherche und Vergleich von Hilfsangeboten bleiben damit jeder Kommune selbst überlassen, was zu Lücken führt.

Fehlende bundeseinheitliche Mindeststandards gefährden letztlich die Informationssicherheit der Kommunen und somit die Daten der Bürgerinnen und Bürger. Ob eine Kommune in IT-Sicherheit investiert, hängt bisher stark vom örtlichen politischen Willen und der Finanzlage ab. In der Praxis konkurriert das Thema mit vielen anderen dringenden kommunalen Aufgaben um Aufmerksamkeit und Mittel. Ohne rechtliche Verpflichtung werden die notwendigen Investitionen und organisatorischen Maßnahmen jedoch häufig nachrangig behandelt.

Eine aktuelle Untersuchung des Cyber Resilience Lab (Resilienzmonitor 2025, abrufbar unter www.resilienzmonitor.de) zeigt, dass das Fehlen organisatorischer Maßnahmen die Auswirkungen von IT-Störungen zusätzlich verschärft. Der Mitteldeutsche Rundfunk (MDR) hat am 12.10.2025 darüber unter anderem unter Bezugnahme auf die IT-Störungen in Potsdam darüber berichtet.[2] Nur 10% der teilnehmenden Kommunen hatten in den letzten 5 Jahren keine IT-Störung. Dies zeigt noch einmal eindrücklich das Ausmaß der Verwundbarkeit.

Eine aktuelle Analyse der Bertelsmann-Stiftung (Kommunaler Finanzreport 2025) zeigt, dass die Kommunen in Deutschland 2024 ein **kumuliertes Defizit von rund 25 Mrd. €** aufweisen – das größte Haushaltsloch in der Geschichte der Bundesrepublik. Die Finanzlage hat sich

[2] https://www.mdr.de/mdr-aktuell-nachrichtenradio/audio/mdr-aktuell-radio-zum-nachhoeren100.html#20251012_9-12 (abgerufen 12.10.2025)

flächendeckend verschlechtert, wodurch **Investitionen in IT-Sicherheit noch unwahrscheinlicher** werden. Kurz gesagt: Wer eine Regulierung ablehnt – vielleicht aus Sorge vor Umsetzungsproblemen – wird kaum in der Lage sein, rein freiwillig die nötigen Sicherheitsmaßnahmen freiwillig einzuführen.

Die **Bürgerinnen und Bürger müssen darauf vertrauen können, dass ihre persönlichen Daten und die kommunalen Dienstleistungen geschützt sind** – unabhängig davon, in welcher Gemeinde sie leben. Anders als bei privaten Online-Diensten oder Firmen haben sie keine Wahl, ob sie einer Behörden-Website oder dem Einwohnermeldeamt ihre Daten anvertrauen - sie müssen es tun, weil staatliche Leistungen ortsgebunden sind und die örtliche und sachliche Zuständigkeit darüber entscheidet wo die Daten erfasst und verarbeitet werden. Im Extremfall bliebe nur ein Umzug in eine „sichere“ Kommune, um beispielsweise das eigene Unternehmen an einem Verwaltungssitz mit geringerer Ausfallwahrscheinlichkeit anzusiedeln. Dies ist unzumutbar, denn es darf nicht vom Wohnort abhängen, ob man vor den Auswirkungen eines Cyberangriffs auf die Verwaltung besser oder schlechter geschützt ist. Ein weiterer Effekt wäre die Abwanderung von Gewerbe und Kaufkraft aus ohnehin strukturschwachen Kommunen, wenn diese sicherheitstechnisch den Anschluss verlieren. Kurzum: Ohne verbindliche Mindeststandards droht eine digitale Zwei-Klassen-Gesellschaft unter den Kommunen.

Dringende Gründe für die Einbeziehung der Kommunen

Angesichts der skizzierten Gefahren und Ungleichheiten sprechen alle Umstände **eindeutig für eine Aufnahme der Kommunalverwaltungen** in den Anwendungsbereich des NIS2UmsuCG:

- **Gesellschaftliche Kritikalität kommunaler Dienste:** Städte, Gemeinden und Landkreise gewährleisten wesentliche Grundversorgungsleistungen (von der Wasserversorgung über Melde- und Gesundheitsämter bis zur Abfallentsorgung). Ein längerer IT-Ausfall in einer Kommune kann ganze Lebensbereiche lahmlegen. Beispiele der letzten Jahre – etwa die Cyberattacke auf die Südwestfalen-IT, die für 72 Kommunen arbeitete – zeigen, dass die Wiederherstellung nach einem schweren Angriff Monate dauern kann. Ein solcher Zustand ist untragbar. Durch präventive Sicherheitsmaßnahmen und Maßnahmen zur Betriebsfortsetzung (BCM) ließe sich das Risiko solcher langanhaltenden Dienstleistungsunterbrechungen deutlich senken.
- **Reale Bedrohungslage gerade für Kommunen:** Wie oben dargelegt, richten sich staatlich geduldete Hackergruppen verstärkt gegen kommunale Ziele. Kommunen sind somit zu einem Frontabschnitt im Cyberraum geworden. Diese Realität erfordert, dass Kommunalverwaltungen denselben Schutzstandard entwickeln wie kritische Unternehmen – im Interesse der nationalen Sicherheit. Andere EU-Länder, die Kommunen ausdrücklich in ihre NIS-2-Umsetzung einbeziehen, begründen dies im Kern mit drei Aspekten:

  (1) die gesellschaftliche Kritikalität der kommunalen Dienste,

(2) der konkreten Bedrohungslage und

(3) dem Bedürfnis nach einheitlichen Mindeststandards, das oft mit einem proportionalen Ansatz kombiniert wird (z. B. abgestufte Pflichten oder mildere Sanktionen für kleinere Einheiten).

Diese Begründungen treffen auch auf Deutschland uneingeschränkt zu.

- **Harmonisierung statt Fragmentierung:** Eine Einbeziehung der Kommunen würde endlich eine dringend notwendige Harmonisierung einleiten und somit die Fragmentierung verhindern. Anstelle von bis zu 16 unterschiedlichen Landesregelungen mit uneinheitlichen Anforderungen, Meldewegen oder Regelungslücken gäbe es einen gemeinsamen Rahmen. Dies würde das derzeit zersplitterte Sicherheitsniveau angleichen und ein **effizienteres Miteinander** von Bund, Ländern und Kommunen in der Cyberabwehr ermöglichen. Angesichts der absehbaren weiteren Verschärfung der Sicherheitslage (Stichworte: steigende Angriffszahlen, komplexere Bedrohungen) ist ein wirkungsorientierter, koordinierter Ansatz zwingend erforderlich. Es braucht eine **einheitliche Abwehrstrategie**, gemeinsame Lagebilder und abgestimmte Mindeststandards auf allen Verwaltungsebenen. Nur so lässt sich ein geschlossenes Schutzschild gegen Cyberangriffe aufbauen.
- **Rechtliche Möglichkeit ist gegeben:** Ein Sachstandsbericht des Wissenschaftlichen Dienstes des Bundestages (EU-6-3000-063/24) hat klargestellt, dass die Aufnahme von Kommunen gemäß Art. 2 Abs. 5 lit. a NIS-2-RL **rechtlich zulässig** ist. Die Frage ist daher nicht, ob die Richtlinie auf Kommunen erstreckt werden darf, sondern ob der Gesetzgeber bereit ist, von dieser Option Gebrauch zu machen. Andernfalls müsste er fachlich tragfähige Gründe nennen können, warum trotz der kritischen Bedrohungslage auf eine solche Ausweitung verzichtet wird – und er müsste bereit sein, die Folgen des Status quo in Kauf zu nehmen. Angesichts der oben dargestellten Risiken fällt es schwer, solche Gründe zu benennen.
- **NIS-2 fordert, was ohnehin notwendig ist:** Die NIS-2-Richtlinie fordert im Grunde nur das, was aus Sicht der IT- und Informationssicherheit ohnehin bereits Stand der Dinge sein sollte. Anforderungen wie ein Management der IT-Risiken, angemessene organisatorische und technische Maßnahmen, regelmäßige Sicherheitsupdates, Notfallvorsorge (Incident Response Pläne) und Aufrechterhaltung des Betriebs (BCM) sind Punkte, die jede Kommune schon jetzt im Eigeninteresse umsetzen müsste. Die Realität zeigt jedoch, dass dies oft nicht geschieht, solange es auf Freiwilligkeit beruht.[3] Eine Einbeziehung der Kommunen würde ihnen den nötigen **Regelungsrahmen** und Rückendeckung geben, um diese Maßnahmen vor Ort durchzusetzen. Kommunale Informationssicherheitsbeauftragte könnten gegenüber ihren Kämmerern und Bürgermeistern auf klare gesetzliche Pflichten verweisen, wodurch sich Umsetzung und Ressourcenbeschaffung erheblich erleichtern würden.

[3] Resilienzmonitor 2025, www.resilienzmonitor.de (abgerufen 12.10.2025)

Zusammenfassend sprechen **sicherheitstechnische, gesellschaftliche und strategische Gründe** dafür, die kommunalen Gebietskörperschaften in den Regelungsumfang der deutschen NIS-2-Umsetzung aufzunehmen. Dies entspricht auch den Forderungen aus Fachkreisen: So hat etwa der Bundesverband IT-Sicherheit (TeleTrusT) in einem offenen Brief den IT-Planungsrat ausdrücklich aufgefordert, den Ausschluss der Kommunen rückgängig zu machen – im Interesse eines angemessenen IT-Sicherheitsniveaus in Deutschland.[4] Es sei erforderlich und dringend geboten, insbesondere die Kommunen gesetzlich zu verpflichten, statt sie pauschal herauszulassen. Würde man der Bitte des IT-Planungsrats folgen, gäbe es weiterhin keinerlei gesetzliche Mindestanforderungen für die kommunale IT-Sicherheit – und dies in einer sich zunehmend verschärfenden Sicherheitslage.

Kommunale Selbstverwaltung und Bundeskompetenzen

Ein häufig vorgebrachtes Bedenken lautet, eine Bundesregelung zur IT-Sicherheit der Kommunen könne die verfassungsrechtlich garantierte kommunale Selbstverwaltung (Art. 28 Abs. 2 GG) verletzen. Dazu ist festzuhalten: Die kommunale Selbstverwaltung gibt den Kommunen zwar weitgehende Freiheit bei der Erledigung örtlicher Angelegenheiten. Allerdings darf der Bund sehr wohl allgemeine Rahmenvorgaben setzen, wie diese Aufgaben wahrzunehmen sind, solange er die Organisationshoheit vor Ort wahrt. Im Bereich der **inneren Sicherheit und der Telekommunikation** besitzt der Bund gemäß Art. 73 Abs. 1 Nr. 10 GG die Gesetzgebungskompetenz. Zudem hat er nach Art. 91c GG eine Koordinierungs- und Standardsetzungskompetenz für die Zusammenarbeit in der Informationstechnik. Diese Kompetenzen können im Rahmen der NIS-2-Umsetzung relevant werden.

Konkret bedeutet dies: Der Bund kann Mindeststandards für die Informationssicherheit definieren (z.B. die Pflicht, bestimmte organisatorische Funktionen einzurichten oder Meldewege einzuhalten), er darf den Kommunen jedoch **nicht vorschreiben**, mit welchen technischen Mitteln oder internen Strukturen sie diese Standards erfüllen. Die Aufnahme der Kommunen in ein Bundesgesetz würde keine vollständige Zentralisierung bedeuten. Die lokale Umsetzung läge weiterhin in kommunaler Hand. Ob eine Kommune ihre IT selbst betreibt, einen IT-Zweckverband gründet oder einen Dienstleister beauftragt, bliebe ihr unbenommen. Vorgeschrieben würde lediglich, dass bestimmte Sicherheitsvorkehrungen eingehalten werden. Darin liegt kein unzulässiger Eingriff, sondern die zulässige Wahrnehmung überörtlicher Schutzgüter (nationale Cyber- und Informationssicherheit, Schutz der Bürgerdaten). Solange die Kernbereiche der Selbstverwaltung – wie die Entscheidung über freiwillige Aufgaben, die Haushaltshoheit etc. – unberührt bleiben, erscheint eine solche Rahmengesetzgebung verfassungsrechtlich vertretbar.

Ein Beispiel ist die Verpflichtung zur Benennung eines Informationssicherheitsbeauftragten (CISO) in jeder Kommune. Diese Verpflichtung greift zwar organisatorisch ein, ist aber durch das übergeordnete Ziel der Aufrechterhaltung kritischer Verwaltungsleistungen und der Cybersicherheit insgesamt gerechtfertigt. Wichtig ist, dass im Gesetz auf die Besonderheiten

[4] https://www.teletrust.de/startseite/news/?tx_ttnews%5Btt_news%5D=1604&cHash=f1ef0aceccae46739a4203b58ae91406 (abgerufen 12.10.2025)

der öffentlichen Hand Rücksicht genommen wird, beispielsweise indem klargestellt wird, dass **Bußgelder gegen Kommunen bei Verstößen nicht verhängt** werden. Das sieht auch die NIS-2-Richtlinie vor: Behörden können von Geldstrafen ausgenommen sein. Stattdessen müssten andere Kontroll- und Sanktionsmechanismen greifen, beispielsweise Berichtsauflagen, Überprüfungen oder notfalls Ersatzvornahmen durch Aufsichtsbehörden. Dies wäre analog zu den Regelungen für Bundesbehörden. Auch dort sind keine Bußgelder vorgesehen, sondern interne Aufsichtsroutinen.

Finanzierung und Umsetzbarkeit

Ein weiterer kritischer Punkt sind die **Kosten für die Umsetzung** von NIS-2-Maßnahmen in den Kommunen. Hierzu ist zunächst festzustellen: Die kommunale IT sollte im eigenen Interesse bereits jetzt dem aktuellen Stand der Technik entsprechen, da andernfalls die Wahrnehmung der Aufgaben und der Schutz der Daten dauerhaft gefährdet sind. Soweit dieser Standard in Einzelfällen noch nicht erreicht ist (etwa gemessen am BSI-Grundschutz), liegt dies oft an lokaler Ressourcenknappheit oder Prioritätensetzung. Die Behebung dieser Versäumnisse kann nicht allein Aufgabe von Bund oder Ländern sein, denn es handelt sich um notwendige Investitionen in die Aufgabenerfüllung, die eigentlich bereits jetzt kontinuierlich hätten erfolgen müssen. Insofern stellt die Verpflichtung zur Nachrüstung keinen unzumutbaren neuen Eingriff in die Selbstverwaltung dar, sondern fordert lediglich das ein, was zur pflichtgemäßen Aufgabenerledigung längst erforderlich war.

Gleichwohl sollte der Bund pragmatisch handeln, um die Kommunen nicht zu überfordern und die Akzeptanz der Regelung zu erhöhen. Die Einrichtung eines finanziellen **Ausgleichsmechanismus** ist zu erwägen. Mit dem Sondervermögen von 500 Mrd. € für Infrastruktur und Klimaneutralität hat die Bundesregierung bereits signalisiert, die nationale Resilienz stärken zu wollen. Ein Teil dieser Mittel könnte gezielt und zweckgebunden für die **IT-Sicherheit der Kommunen** eingesetzt werden. Denkbar wäre etwa ein kommunales Cyber-Sicherheitsprogramm, das Investitionen in Basissicherheitsmaßnahmen fördert. Dadurch ließe sich der Vorwurf entkräften, der Bund lasse die Kommunen mit den Kosten allein. Zugleich würde ein solches Programm die Bedeutung kommunaler Leistungen für den Gesamtstaat unterstreichen und ein klares Signal senden, dass die Sicherheit der Bürgerdaten überall Priorität hat.

Laut Schätzungen im Referentenentwurf der Bundesregierung würden sich bei Einbeziehung der Kommunen jährliche Mehrkosten in Höhe von **0,8 bis 1,1 Mrd. €** ergeben (abhängig von den zugrunde gelegten Standards und der Einordnung nach Gemeindegrößen). Dieser Betrag mag hoch klingen, er relativiert sich jedoch angesichts der Schäden, die durch einzelne erfolgreiche Cyberangriffe entstehen können (man denke an Lösegeldzahlungen, Wiederaufbaukosten und wirtschaftliche Folgeschäden durch Behördenausfälle). Zudem reduzieren Synergieeffekte und zentral bereitgestellte Lösungen – beispielsweise ein einheitliches Bund-Länder-Meldeportal für Sicherheitsvorfälle, das zentral vom BSI betrieben wird – den Aufwand auf kommunaler Seite. Die einmaligen **Initialkosten** für organisatorische Anpassungen und Schulungen wurden auf etwa einen Jahressatz der laufenden Kosten, also ebenfalls 0,8 bis 1 Mrd. €, geschätzt. Angesichts der Bedeutung der Aufgabe erscheint diese

Investition in die Resilienz der Verwaltung gerechtfertigt und finanzierbar – zumal sie auf über 10.000 Kommunen verteilt wird.

Ein weiterer wichtiger Aspekt ist die **Umsetzungsfrist**. Unternehmen, die neu unter NIS-2 fallen, haben in der Regel ab Inkrafttreten der Richtlinie 21 Monate Zeit, um die Vorgaben umzusetzen. Kommunen hingegen wurden bislang ausgenommen und hätten im Falle einer nachträglichen Einbeziehung keine vorbereitende Übergangsphase genossen. Es wäre daher fair und sinnvoll, im Gesetz auskömmliche Übergangsregelungen für Kommunalverwaltungen vorzusehen, beispielsweise gestaffelte Fristen abhängig von der Gemeindegröße. Allerdings sollten diese Übergangszeiten **nicht für die Meldepflichten** gelten. Die Fähigkeit, Sicherheitsvorfälle zu melden, sollte so schnell wie möglich aufgebaut werden, da nur mit lückenlosen Meldungen ein umfassendes und aktuelles Lagebild erstellt werden kann. Die technischen Voraussetzungen dafür – insbesondere eine zentrale Meldestelle beim BSI – müssen ohnehin kurzfristig geschaffen werden. Hier könnte man höchstens pragmatische Lösungen für die Anfangszeit erwägen (z. B. niederschwellige Meldewege).

Selbstverständlich muss darauf geachtet werden, die **zusätzliche Bürokratiebelastung** gering zu halten. Standardisierte Verfahren, Leitfäden und Muster von Bund und Ländern können dabei helfen, dass die Kommunen das Rad nicht neu erfinden müssen. Eine föderal differenzierte Herangehensweise schließt diese Unterstützung durch den Bund nicht aus, im Gegenteil: Sie wird umso wichtiger, wenn kleine Kommunen verpflichtet werden. Wichtig ist jedoch, dass **Sicherheit Vorrang** vor Bequemlichkeit hat. Angesichts der Risiken wäre es falsch, aus Angst vor administrativem Mehraufwand auf notwendige Maßnahmen zu verzichten. Der Schlüssel liegt vielmehr darin, Pflichten **zielführend umzusetzen**: mit digitaler Unterstützung, wo möglich, und in enger Abstimmung zwischen Bund, Ländern und kommunaler Ebene, um Doppelstrukturen zu vermeiden.

Empfehlung: Ich empfehle ausdrücklich, den Anwendungsbereich des NIS2UmsuCG auf die Kommunen zu erstrecken und die dafür erforderlichen gesetzlichen Grundlagen zu schaffen. Die Kommunalverwaltungen sollten ebenso wie wesentliche Unternehmen verpflichtet werden, Mindeststandards der IT- und Informationssicherheit einzuhalten. Dies würde eine einheitliche Abwehrstrategie ermöglichen, gemeinsame Lagebilder schaffen und föderale Cyber-Sicherheitsaktivitäten besser verzahnen. Die aktuell **vorgesehene Ausklammerung kommunaler Einrichtungen** birgt die Gefahr, dass ein großer Teil der staatlichen IT-Infrastruktur ungeschützt bleibt. Diese Fragmentierung der nationalen Cyber-Architektur erhöht die Risiken für das Gesamtsystem. Bund und Länder sollten hier gemeinsam gegensteuern. Sollte der Bund tatsächlich – wie im Planungsrat beschlossen – keine direkte Regelung treffen, müssen zumindest die Länder motiviert werden, kommunale Stellen in entsprechende Landesgesetze einzubeziehen, um die strukturelle Deckungslücke zu schließen. Insgesamt wäre ein bundeseinheitliches Vorgehen jedoch effizienter und klarer.

Melde- und Registrierungspflichten effizient gestalten

Ein Kernanliegen der NIS-2-Richtlinie ist es, **Meldewege zu bündeln** und den bürokratischen Aufwand zu reduzieren. Der Gesetzentwurf sieht richtlinienkonform das BSI als zentrale

Meldestelle für IT-Sicherheitsvorfälle vor. Diese Bündelung wird von vielen Seiten begrüßt, auch von der Bundesdatenschutzbeauftragten (BfDI), denn sie schafft einen One-Stop-Shop für Meldungen. Ideal wäre es, wenn meldepflichtige Unternehmen und Stellen **Sicherheitsvorfälle mit gleichzeitigem Personenbezug** in einem Vorgang melden könnten, anstatt getrennte Meldungen an das BSI und an die Datenschutzaufsichtsbehörden absetzen zu müssen. Erwägungsgrund 106 der NIS-2-Richtlinie regt explizit dazu an, auf nationaler Ebene integrierte Meldeprozesse zu schaffen. Sofern die Länder hier eigene Verpflichtungen geschaffen haben, gilt es, diese zu integrieren oder von vornherein die Möglichkeit zur Integration zu schaffen.

Dabei ist auf **die Abstimmung der Meldewege** zu achten. Viele Experten – darunter auch der Bundesrat – haben kritisiert, dass es für meldepflichtige Unternehmen und Stellen nicht zumutbar ist, denselben Vorfall mehrfach an verschiedene Stellen mit unterschiedlichen Formularen zu melden. Im schlimmsten Fall muss ein Unternehmen heute beispielsweise an das BSI, an einen Landes-CERT, an die BfDI und an eine Landes-Datenschutzbehörde separat berichten – und das unter Zeitdruck, während die IT gegebenenfalls noch ausgefallen ist. Ziel muss ein **abgestimmtes Meldewesen** sein, das Doppelmeldungen ausschließt. Das zentrale Bundesportal sollte so konzipiert sein, dass es die relevanten Informationen auf Wunsch automatisiert an alle zuständigen Stellen weiterverteilt. Länder, die eigene Meldeportale betreiben, sollten umgekehrt verpflichtet werden, Meldungen **unverzüglich ans BSI weiterzuleiten**, damit das gesamtstaatliche Lagebild vollständig bleibt. Es darf nicht passieren, dass föderale Eifersüchteleien den Informationsfluss hemmen. Hier ist Kooperation gefragt. Der Gesetzentwurf legt mit § 40 BSIG-E eine Grundlage, doch die praktische Ausgestaltung muss in **Verwaltungsvereinbarungen** zwischen Bund und Ländern festgelegt werden. Hierzu gibt es bereits Gespräche: Der IT-Planungsrat hat die AG Informationssicherheit beauftragt, die Abstimmung zu dieser Frage fortzuführen. Diese Bemühungen müssen konsequent weiterverfolgt werden, um spätestens bis zum Inkrafttreten des Gesetzes eine **technische und organisatorische Meldeinfrastruktur** bereitzuhaben, die für alle Meldepflichtigen einen echten Mehrwert bringt, nämlich weniger Aufwand und mehr Sicherheit durch gebündelte Informationskanäle.

In der ersten Entwurfsrunde hatte der Bundesrat vorgeschlagen, dem BSI die Aufgabe zu geben, **kombinierte Meldungen** entgegenzunehmen und die Angaben, die eine Datenschutzverletzung betreffen, automatisiert an die zuständigen Datenschutzbehörden weiterzuleiten. Dies hätte den Vorteil, dass ein betroffener Betreiber nur einmal einen Vorfall beschreibt und alle relevanten Stellen informiert sind. Die Bundesregierung hat diesen Vorschlag im vorliegenden Entwurf jedoch nicht übernommen und dies mit juristischen Hürden begründet. So enthalte Art. 33 DSGVO (Meldepflicht bei Datenschutzverletzungen) keine Öffnungsklausel, die eine Meldung an andere Stellen erlaubt. Zudem wurde auf das Verbot der Mischverwaltung hingewiesen, falls eine Bundesbehörde (BSI) Aufgaben für Landesdatenschutzbehörden übernehmen würde.

Diese Einwände sind formal zutreffend, sie sollten jedoch **umgangen** werden, um das Ziel trotzdem zu erreichen. Die BfDI hat hierzu ein zweistufiges Konzept vorgeschlagen:

Zunächst könnte das BSI zumindest technische Verfahren anbieten, mit denen ein Meldepflichtiger **gleichzeitig** seine NIS-2-Meldung und seine DSGVO-Meldung erstellen kann. Konkret könnte das BSI-Portal so angepasst werden, dass es aus den eingegebenen Vorfallsdaten automatisch einen voradressierten Bericht an die Datenschutzbehörde generiert, den das Unternehmen nur noch absenden muss. Juristisch bliebe die DSGVO-Meldung damit in der Hand des Verantwortlichen, da die Meldung nicht vom BSI selbst versandt würde, um eine Mischverwaltung zu vermeiden. Dennoch würde dieses Verfahren die praktische Doppelbelastung nahezu eliminieren. **Langfristig** sollte sich Deutschland zudem auf EU-Ebene dafür einsetzen, die datenschutzrechtlichen Vorgaben so zu ändern, dass ein vollintegrierter Meldeprozess möglich wird. Bis dahin ist die skizzierte Lösung ein gangbarer Kompromiss. Ich unterstütze daher die Empfehlung, in § 40 BSIG-E eine Klausel aufzunehmen, die das BSI dazu verpflichtet, geeignete Verfahren für gebündelte Meldungen bereitzustellen. Dies würde Unternehmen und Behörden spürbar entlasten, ohne den Schutz personenbezogener Daten zu schmälern.

Ein weiterer wichtiger Aspekt ist die **Meldepflicht für Kommunen**, falls diese in den Anwendungsbereich aufgenommen werden. Derzeit ist die Situation heterogen: Einige Länder (Bayern, Baden-Württemberg und Sachsen) haben in ihren Landesgesetzen bereits Vorgaben, wonach Kommunen IT-Sicherheitsvorfälle an das Landes-CERT oder das Innenministerium melden müssen. Andere Länder – wie beispielsweise Nordrhein-Westfalen im Entwurf seines IT-Sicherheitsgesetzes – sehen hingegen keine Meldepflicht für Kommunen vor. Faktisch sind Kommunen jedoch bereits jetzt dazu verpflichtet, **Datenschutzverletzungen** innerhalb von 72 Stunden an die Datenschutz-Aufsichtsbehörde zu melden (Art. 33 DSGVO). Viele Cybervorfälle ziehen eine solche Verletzung nach sich. Dennoch gelangen technische Details des Vorfalls oft nicht an die Sicherheitsbehörden. In Ländern ohne Meldepflicht erfährt das eigene Landes-CERT beispielsweise nichts vom Vorfall. Dadurch geht wertvolles **Präventionswissen** verloren, da andere Kommunen nicht gewarnt werden können. Das Fehlen einheitlicher Meldeverpflichtungen führt also zu blinden Flecken im Lagebild und mindert die Abwehrmöglichkeiten aller.

Mit einer bundeseinheitlichen, verpflichtenden Meldestruktur, die beim BSI angesiedelt ist, ließe sich dagegen **zeitnah ein umfassendes kommunales Lagebild** erstellen. Diese Aufgabe und Zuständigkeit sollte dem BSI im Gesetz eindeutig zugewiesen werden. Das BSI kann eingehende Meldungen auswerten und beispielsweise über seinen Warn- und Informationsdienst, wie er bereits für KRITIS-Unternehmen etabliert wurde, gezielt vor aktuellen Bedrohungen warnen. Wichtig ist allerdings: Der **Mehrwert der Meldungen muss für beide Seiten bestehen**. Es reicht nicht aus, wenn Kommunen pflichtgemäß Vorfälle melden, die Daten aber im „Meldungsfriedhof“ verschwinden. Die meldenden Stellen müssen unmittelbar von den gewonnenen Erkenntnissen profitieren, beispielsweise durch **zeitnahe Rückmeldungen, Warnungen und Hilfestellungen**. Hierzu sollte das BSI ein spezielles Informationsangebot für die öffentliche Verwaltung aufbauen bzw. ausweiten. Denkbar wäre beispielsweise ein **kommunales Cyber-Lagezentrum** beim BSI. Dieses analysiert die gemeldeten Vorfälle und stellt den Kommunen sowohl aktive Informationen (Warnungen, Handlungsanweisungen) als auch interaktive Elemente bereit. Hierzu zählt etwa

der Zugriff auf ein Dashboard mit aktuellen Angriffsmustern oder Schwachstellen, das auf den Verwaltungsbereich abgestimmt ist. Der oft geäußerten Befürchtung, kleine Kommunen könnten ein Cyber-Lagebild nicht „interpretieren", muss dadurch begegnet werden, dass die Inhalte adressatengerecht aufbereitet und zugänglich gemacht werden. Der Informationsbedarf ist eindeutig vorhanden und muss durch das BSI gedeckt werden.

Einheitliche Sicherheitsstandards für die Bundesverwaltung

Der Regierungsentwurf setzt in Bezug auf die **Bundesverwaltung** leider ein inkonsistentes Schutzniveau an. Zwar werden erstmals auch Bundesbehörden verpflichtet, ein Informationssicherheits-Management umzusetzen, was ausdrücklich zu begrüßen ist. Der Entwurf enthält jedoch eine Unterscheidung zwischen den obersten Bundesbehörden (Bundeskanzleramt und Bundesministerien) und der übrigen Bundesverwaltung. Letztere sollen beispielsweise nicht verpflichtet sein, ein vollumfängliches **Risikomanagement nach § 30 BSIG-E** durchzuführen und den BSI-Grundschutz als Standard zu erfüllen. Alle nachgeordneten Behörden (bis hin zu den Bundesober- und -mittelbehörden) müssen dagegen lediglich die einfacheren **Mindeststandards** des BSI umsetzen. Diese Zweiteilung schafft ein **IT-Sicherheitsgefälle** innerhalb der Bundesverwaltung, das sich sachlich kaum rechtfertigen lässt. Auch das BSI selbst sieht ein einheitliches Cyber-Sicherheitsniveau für die gesamte Bundesverwaltung als zwingend erforderlich an.

Mehrere Risiken ergeben sich aus der aktuellen Fassung:

- **Einfallstor-Funktion:** Alle Bundesbehörden sind vernetzt und tauschen Daten. Teilweise nutzen sie gemeinsame Netze und Dienste. Wenn nun Bundesbehörden nur ein Minimalniveau an Sicherheit haben, könnten sie als Einfallstor für Angreifer dienen, um sich seitlich zu wichtigeren Zielen vorzuarbeiten. Ein gezielter Angriff sucht sich immer das schwächste Glied.
- **Ungleichbehandlung gegenüber der Wirtschaft:** Wesentliche und wichtige Unternehmen der Privatwirtschaft müssen nach NIS-2 sehr weitgehende Maßnahmen umsetzen, bis hin zu externen Audits. Es ist kaum vermittelbar, warum ausgerechnet Bundesbehörden hier unter diesem Niveau bleiben sollen. Der Ruf nach Gleichbehandlung ist laut: Der Staat sollte mit gutem Beispiel vorangehen und nicht hinterherhinken.
- **Intransparenz und Verantwortungsdiffusion:** Der Entwurf sieht vor, dass die Behördenleitungen vieler Bundesbehörden von den strikten persönlichen Verantwortlichkeiten (z. B. Billigung des Sicherheitskonzepts, Schulungspflichten) ausgenommen sind. Zudem sollen die Behörden – anders als Unternehmen – keinen regelmäßigen externen Prüfungen unterliegen, sondern nur alle fünf Jahre eine Eigenerklärung abgeben. Dies mindert den Handlungsdruck erheblich. Ohne externen Blick und ohne persönliche Rechenschaft der Führung bleibt zu befürchten, dass Sicherheitsthemen in der Verwaltung nachrangig behandelt werden.

Um diese Probleme zu beheben, schlage ich folgende **Änderungen** vor:

- **Gleiches Sicherheitsniveau für alle Bundesbehörden:** Die Unterscheidung zwischen obersten Bundesbehörden und dem Rest in § 29 und § 44 BSIG-E sollte gestrichen werden. Sämtliche Bundesbehörden müssen vergleichbare Sicherheitsmaßnahmen umsetzen. Insbesondere sollte die Pflicht zur Einführung eines Informationssicherheitsmanagementsystems (ISMS) nach § 30 BSIG-E und zur **Umsetzung des BSI-Grundschutzes** nicht nur für Ministerien, sondern für alle gelten. Dies würde das Niveau der Bundes-IT signifikant anheben und für konsistente Sicherheit sorgen.
- **Einschränkung von Ausnahmeregelungen:** Der Entwurf ermöglicht es in § 37 BSIG-E dem Bundesinnenministerium, dem Kanzleramt, dem Justiz-, Verteidigungs- oder Finanzministerium, bestimmte Einrichtungen per Bescheid ganz oder teilweise von den Pflichten auszunehmen. Hier ist große Zurückhaltung geboten. Jede Ausnahme schwächt die Gesamtsicherheit und kann erhebliche Lücken reißen. Wenn etwa Strafverfolgungsbehörden oder das Auswärtige Amt (mit Verweis auf besondere Geheimhaltungserfordernisse) aus weiten Teilen des Gesetzes ausgenommen würden, bestünde die Gefahr, dass Angreifer genau dort ansetzen. Notwendige Ausnahmen – etwa für die Nachrichtendienste oder militärische Stellen – sollten eng begrenzt und mit Kompensationsmaßnahmen versehen werden. Pauschale Freistellungen widersprechen dem Ziel eines hohen gemeinsamen Sicherheitsniveaus. **Grundsatz:** Ausnahmen sollten so selten und so eng wie möglich sein, um die Glaubwürdigkeit und Wirksamkeit der Regulierung nicht zu untergraben.
- **Verantwortung der Behördenleitung verankern:** Führungskräfte in Behörden sollten ähnlich wie Unternehmensvorstände für die Cybersicherheit in ihrem Verantwortungsbereich einstehen. Daher ist zu überlegen, die Pflichten zur strategischen Steuerung (Billigung der Sicherheitskonzepte, regelmäßige Lagevorträge usw.) auf alle Leitungsebenen auszuweiten. Nur wenn die Spitze einer Behörde das Thema aktiv vorlebt, wird es in der Organisation ernst genommen. Haftungs- oder Disziplinarfragen spielen im öffentlichen Dienst zwar eine andere Rolle als in Unternehmen, aber zumindest eine klare Zuweisung von Verantwortlichkeit (z. B. in Geschäftsordnungen der Ministerien) wäre förderlich. Dies impliziert auch die erforderlichen verpflichtenden Schulungen für Behörden, die mit denen für Geschäftsführungen vergleichbar sind.
- **Externe Überprüfung und kürzere Nachweisintervalle** sind ebenfalls erforderlich, da die Glaubwürdigkeit der Umsetzung leidet, wenn Bundesbehörden ihre Sicherheit weitgehend selbst attestieren. Anstelle einer reinen Eigenerklärung alle fünf Jahre sollte – analog zur Privatwirtschaft – ein verpflichtender **Überprüfungszyklus** von drei Jahren in Betracht gezogen werden. Dieser Check kann durch unabhängige Auditoren erfolgen. Wichtig ist, dass eine objektive Evaluierung stattfindet. Die Prüfer sollten rotieren und nicht durch Rahmenverträge dauerhaft an eine Behörde gebunden sein. Eine solche „Prüf-Schleife" würde den Umsetzungsdruck deutlich erhöhen und zugleich dem Parlament und der Öffentlichkeit Sicherheit geben, dass die Behörden ihrer Pflicht auch tatsächlich nachkommen.

In seiner Stellungnahme plädiert das BSI ausdrücklich für diese Punkte und sieht hierin den größten kurzfristigen Hebel, um die Bundes-IT resilienter zu machen. Besonders hervorgehoben wird, dass das Zusammenspiel mit einem zentralen Sicherheitskoordinator (CISO Bund) entscheidend ist, um die Verbesserungen stringent umzusetzen. Hierzu mehr im nächsten Abschnitt. Insgesamt sollte der Innenausschuss deutlich machen, dass die derzeitige Schwächung der Pflichten für die Bundesverwaltung nicht akzeptabel ist. Der ursprüngliche Referentenentwurf sah in einigen Punkten strengere Regeln vor (z. B. Nachweis in drei Jahren); diese sollten wieder aufgegriffen werden. Die Bundesverwaltung darf nicht hinter den Standard zurückfallen, den man von Wirtschaft und Gesellschaft verlangt. Gerade auch mit Blick auf die aktuellen Spionage- und Sabotagegefahren (Stichworte: **Bundeswehr und Auswärtiges Amt**, die bekanntlich im Fokus ausländischer Dienste stehen) muss der Staat maximal wehrhaft aufgestellt sein.

Positiv anzumerken ist, dass der Entwurf die Möglichkeit von Buß- und Zwangsgeldern gegen Behörden gar nicht erst vorsieht. NIS-2 lässt hier Spielraum und es ist vernünftig, auf rein verwaltungsinterne Mechanismen zu setzen, statt staatliche Stellen mit Geldstrafen zu überziehen. Umso wichtiger ist dann aber die hier geforderte interne Kontrolle und Rechenschaft, damit die Regelungen nicht zahnlos bleiben.

Stärkung der Unabhängigkeit des BSI

Die Unabhängigkeit des BSI muss gestärkt werden, denn eine starke, kompetente und **unabhängige nationale Cyber-Sicherheitsbehörde** ist ein zentrales Element erfolgreicher Cyber-Sicherheitspolitik. Die NIS-2-Richtlinie fordert explizit, dass die zuständigen Stellen über ausreichende Ressourcen verfügen und ihre Aufgaben **unparteiisch und frei von unzulässiger Einflussnahme** erfüllen können. In Deutschland nimmt das Bundesamt für Sicherheit in der Informationstechnik (BSI) diese Rolle wahr. Allerdings ist das BSI derzeit organisatorisch dem Bundesministerium des Innern (BMI) unterstellt und unterliegt dessen Fachaufsicht. Die neue Bundesregierung hatte im Koalitionsvertrag von 2021 angekündigt, das BSI zu einer „unabhängigeren“ Behörde auszubauen (Stichwort: Herauslösung aus dem BMI). Bisher ist dies jedoch nicht umgesetzt worden – auch der NIS2UmsuCG-Entwurf enthält dazu keinerlei Regelungen.

Diese Untätigkeit ist zu kritisieren. Die NIS-2-Richtlinie verlangt eine operative Unabhängigkeit – hier besteht Nachholbedarf. Die Unabhängigkeit des BSI ist wichtig, da sowohl Vertrauen als auch Effektivität auf dem Spiel stehen. Das BSI soll als nationale Cyber-Abwehrzentrale agieren und erhält durch NIS 2 zahlreiche neue Befugnisse und Aufgaben. Gleichzeitig darf nicht der Eindruck entstehen, dass es politischen Weisungen folgt, Informationen zurückhält oder Entscheidungen nach politischer Opportunität trifft. Für Bürgerinnen und Bürger sowie für die Wirtschaft ist es entscheidend, dass das BSI **neutral, transparent und fachlich motiviert** handelt.

Der Gesetzentwurf hätte hier zumindest **strukturelle Klarstellungen** treffen sollen. Denkbar wäre beispielsweise eine Regelung, die festschreibt, dass das BSI im Rahmen seiner Aufgaben weisungsfrei agiert, soweit es der Cybersicherheit dient. Konkret könnte folgende Regelung

aufgenommen werden: „Weisungen, die der Erfüllung der Cyber-Sicherheitsaufgaben zuwiderlaufen, sind unzulässig." Eine solche Formulierung würde sicherstellen, dass gemeldete Schwachstellen immer der Schließung zugeführt werden und **keine Weisung** erteilt werden kann, dies zu unterbinden. Dieses allgemeine Prinzip ließe sich auch auf andere Bereiche ausdehnen. Zusätzlich sollte das BSI verpflichtet werden, regelmäßig gegenüber dem Parlament Bericht zu erstatten, beispielsweise in Form **eines jährlichen Lageberichts** zur Sicherheit in den nach NIS-2 regulierten Bereichen (ähnlich dem BSI-Lagebericht zur Cybersicherheit, jedoch erweitert um die Aspekte Bundesbehörden und Umsetzung der NIS-2-Pflichten). Dies würde eine **parlamentarische Kontrolle** ermöglichen und Transparenz schaffen, wo der Gesetzentwurf bislang Schweigen bewahrt.

Ein weiterer Punkt ist die **Durchsetzungsbefugnis des BSI** gegenüber anderen Bundesbehörden. Zwar verankert der Entwurf, dass das BSI gegenüber den Bundesstellen Anordnungen treffen kann, um akute Sicherheitsvorfälle abzuwehren (§ 10 BSIG-E), doch in der Praxis wird das BSI hier vorsichtig agieren, solange es nicht wirklich unabhängig ist. In der Praxis wird das BSI jedoch nur vorsichtig agieren, solange es nicht wirklich unabhängig ist. Es ist daher zu überlegen, ob dem BSI – analog zu seiner Rolle bei KRITIS-Unternehmen – eine verpflichtende Aufgabe zur regelmäßigen **Überprüfung** der Bundesbehörden übertragen werden sollte (z. B. Penetrationstests oder Audits nach einem stufenweisen Plan). Solange solche Prüfungen nur „nach Gutdünken" erfolgen, besteht die Gefahr, dass aus Ressourcenmangel wenig passiert. Wäre es hingegen eine klar definierte Pflicht inklusive Finanzierungszusage, hätte das BSI sowohl den Auftrag als auch die Mittel, tatsächlich flächendeckend aktiv zu werden.

Empfehlung: Das Gesetz sollte die Stellung des BSI als Implementierungsbehörde nach NIS-2 stärker untermauern. Mindestens sollte ein Passus aufgenommen werden, der dem BSI vorschreibt, ihm gemeldete Schwachstellen unverzüglich an die Hersteller weiterzugeben. Darüber hinaus sollte die Bundesregierung die im Koalitionsvertrag avisierte Reform nicht länger aufschieben. NIS-2 bietet die Gelegenheit, das BSI **rechtlich abgesichert** unabhängiger zu stellen. Diese Chance sollte genutzt werden, um Vertrauen zu schaffen und europäischen Vorgaben zu genügen.

Etablierung eines zentralen CISO Bund

Der Entwurf erwähnt an einigen Stellen einen neuen Akteur: den Koordinator oder die Koordinatorin für Informationssicherheit des Bundes („**CISO Bund**"). Laut Begründung soll damit eine zentrale Steuerungsfunktion geschaffen werden, die die verschiedenen Aktivitäten in den Ressorts koordiniert. Dies ist grundsätzlich eine sehr sinnvolle Idee, da in Zukunft in jedem Ressort ein eigener IT-Sicherheitsbeauftragter (Ressort-CISO) benannt werden muss. Ohne **zentralen Zusammenhalt** besteht die Gefahr von Ressortegoismen, dass also jeder sein eigenes Süppchen kocht. Ein CISO Bund könnte hier für einheitliche Standards sorgen und als Eskalationsinstanz dienen, wenn irgendwo gravierende Mängel auftreten.

Problematisch ist jedoch, dass der Gesetzentwurf die Rolle kaum ausfüllt. Weder werden konkrete Aufgaben noch Befugnisse des CISO Bund im Gesetz definiert. Offenbar soll dies per

Kabinettsbeschluss oder organisatorisch im Nachgang geregelt werden. Diese Unbestimmtheit lässt befürchten, dass der CISO Bund lediglich eine symbolische Koordinationsrolle ohne **echte Durchgriffsrechte** erhält. Der Bundesrechnungshof hat bereits angemerkt, dass klare Pflichten und Befugnisse fehlen, um ressortübergreifend eine einheitliche Steuerung der Cybersicherheit zu ermöglichen.

Um die Wirksamkeit zu gewährleisten, müssen folgende Aspekte beachtet werden:

- **Klare Verankerung im Gesetz:** In § 3 BSIG-E (Aufgaben des BSI) oder einem eigenen Paragrafen sollte ausdrücklich festgeschrieben werden, dass das BSI die Funktion eines CISO Bund übernimmt. Das BSI selbst schlägt vor, die Leitung des BSI mit dieser Aufgabe zu betrauen. Damit wäre die Position direkt in die bestehende Struktur integriert. Alternativ könnte der CISO Bund als Stabsstelle beim Bundeskanzleramt angesiedelt werden, um eine noch höhere Unabhängigkeit vom Innenressort zu erreichen. Wichtig ist aber, dass kein zusätzlicher „Wasserkopf" entsteht, sondern der CISO Bund in der Lage ist, operativ Einfluss zu nehmen.
- **Notwendige Befugnisse:** Ein CISO Bund braucht das Recht, verbindliche **bundesweite Sicherheitsprogramme** zu entwickeln, Vorgaben zu machen und deren Umsetzung zu überwachen. Der BSI-Vorschlag sieht beispielsweise vor, dass der CISO Bund Programme zur Gewährleistung der Informationssicherheit erstellt und fortschreibt – im Benehmen mit den Ministerien – und deren Umsetzung durch die BSI-Befugnisse überwacht. Außerdem soll er jährlich dem Bundestag (Haushaltsausschuss) über den Umsetzungsstand berichten. Diese Punkte sollten im Gesetz verankert werden, um der Rolle Kontur zu geben.
- **Anbindung und Unabhängigkeit:** Der CISO Bund sollte möglichst hoch angesiedelt sein. Denkbar ist eine Zuordnung als Stabsstelle zum Bundeskanzleramt, um das Querschnittsanliegen zu betonen. Wichtig ist, dass die Stelle genügend Autorität hat, um auch gegenüber Staatssekretären und CIOs der Ministerien Gehör zu finden. Zudem muss die Rolle **fachlich unabhängig vom CIO Bund** agieren können. Nur so sind Checks and Balances gewährleistet. Idealerweise wäre der CISO-Bund rangmäßig dem CIO-Bund gleichgestellt oder übergeordnet.
- **Koordination vs. Kontrolle:** Der CISO Bund sollte nicht als Konkurrenz zum BSI oder zu den Ressorts verstanden werden, sondern als fehlendes Bindeglied. Er/sie kann beispielsweise dafür sorgen, dass alle Ressorts bei der Umsetzung des IT-Grundschutzes vergleichbar vorankommen, Hindernisse identifiziert und adressiert werden (notfalls auch politisch). Man könnte die Stelle mit einem Weisungsrecht in Krisenfällen ausstatten, um bei einem übergreifenden Sicherheitsvorfall zentral Maßnahmen anordnen zu können. Der CISO Bund sollte auch befugt sein, bei Nachlässigkeiten in einzelnen Behörden Alarm zu schlagen und das Thema notfalls in die Chefetage (Kanzleramt) zu tragen. Zudem obliegt dem CISO Bund die Abstimmung mit den Landesstellen.
- **Keine Doppelstrukturen:** Wichtig ist, dass der CISO Bund eng mit dem BSI verzahnt wird.

Zusammengefasst ist ein **unabhängiger, kompetenter CISO Bund unverzichtbar**, um die IT-Sicherheit in der Bundesverwaltung ganzheitlich zu steuern. Derzeit lässt der Entwurf diese Stelle im Unklaren – das sollte dringend nachgebessert werden. Hier bietet sich eine gute Gelegenheit, die in der Vergangenheit oft monierte fehlende Gesamtkoordination zu beheben. Es gab beispielsweise früher keinen zentralen Sicherheitsverantwortlichen für den Bund, was als Mangel galt.

Klar geregelter Umgang mit IT-Schwachstellen

Ein klar geregelter Umgang mit IT-Schwachstellen ist besonders wichtig. Im aktuellen Entwurf ist dieser Umgang jedoch **nicht ausreichend geregelt**. Seit Jahren wird darüber diskutiert, wie sich staatliche Stellen verhalten sollen, wenn ihnen Sicherheitslücken bekannt werden, etwa durch Meldungen von Forscher:innen oder eigene Entdeckungen. Die Frage ist: Soll die Sicherheitslücke geschlossen oder für staatliche Zwecke genutzt werden? Das Bundesverfassungsgericht hat dem Gesetzgeber in seinem „Hackback"-Urteil (zum Staatstrojaner) explizit aufgegeben, für den Umgang mit sogenannten Zero-Day-Schwachstellen Regeln zu finden. Dennoch enthält der NIS2UmsuCG keinen solchen Passus, obwohl er viele andere Aspekte der Cybersicherheit adressiert.

Meine Position ist klar: **Jede Schwachstelle muss so schnell wie möglich geschlossen werden.** Nur so ist die Allgemeinheit geschützt und das Vertrauen in digitale Dienste bleibt erhalten. Das Offenhalten von Sicherheitslücken für Polizei- oder Geheimdienstzwecke mag in Einzelfällen verlockend erscheinen, erzeugt aber immer **Kollateralschäden**. Denn die Lücke bleibt für alle Angreifer nutzbar, nicht nur für „die Guten". Dadurch wird die Sicherheit aller Nutzer eines Produkts geschwächt, nicht nur die der Zielperson eines staatlichen Eingriffs.

Der Gesetzentwurf verpasst die Chance, hier klare Leitplanken einzuziehen. Er lässt offen, was mit den beim BSI gemeldeten Schwachstellen geschieht. Zwar betont die BSI-Präsidentin, dass ihr Haus selbst keine Lücken offenhalte, doch die Ungewissheit, ob gemeldete Schwachstellen möglicherweise an Strafverfolgungsbehörden weitergereicht oder anderweitig genutzt werden, schreckt Sicherheitsforscher ab. Hier ergeben sich auch Zuständigkeitskonkurrenzen, beispielsweise mit der Zentralen Stelle für Informationstechnik im Sicherheitsbereich (ZITiS). Viele „White Hats" zögern, Funde zu melden, wenn sie befürchten müssen, dass ihre Entdeckung am Ende gegen Nutzer eingesetzt wird, statt zu einem Patch zu führen. Die Problematik der potenziellen eigenen Strafbarkeit wird dabei noch nicht beleuchtet.

Ich plädiere daher dafür, klar zu regeln, dass **gemeldete Schwachstellen vom BSI niemals zurückgehalten, sondern stets der Schließung zugeführt werden**. Konkret könnte folgender Satz aufgenommen werden: „Das BSI gibt Informationen über gemeldete Schwachstellen unverzüglich an die Hersteller oder verantwortlichen Stellen weiter, damit diese die Schwachstelle schließen können." Eine solche Vorschrift würde unmissverständlich klarstellen, dass das BSI keine Exploits hortet, sondern die Interessen der IT-Sicherheit über alles stellt.

Natürlich bleibt die Situation denkbar, dass eine Sicherheitsbehörde eine unbekannte Lücke entdeckt, beispielsweise in der Software von Kriminellen (man denke an eine Ransomware). Hier argumentieren manche, dass man diese Lücke ausnutzen sollte, um den Kriminellen zu schaden oder Daten zu retten, statt sie zu melden. Solche Szenarien sind jedoch äußerst selten und können nicht die generelle Handlungsmaxime umkehren. Sollte tatsächlich einmal ein solcher Spezialfall eintreten, könnte ein **unabhängiges Gremium** entscheiden, ob temporär von der Regel „Fix it“ abgewichen wird. Wichtig wäre, dass das BSI als Hüter der Sicherheit bei solchen Entscheidungen eingebunden ist, damit die Perspektive der IT-Sicherheit stets vertreten ist. Darüber hinaus verstößt das Ausnutzen einer solchen Schwachstelle zur unmittelbaren operativen Schädigung der Angreifer oder deren IT-Infrastruktur regelmäßig gegen geltendes Völkerrecht[5]

Zusätzlich zum Prozedere sollte auch die **rechtliche Absicherung für Hinweisgeber** verbessert werden. Das Strafrecht (§§ 202a StGB ff., sogenannte Hackerparagraphen) ist derzeit so gefasst, dass sich selbst gutwillige Sicherheitsforscher unter Umständen strafbar machen, wenn sie eine Schwachstelle erkunden. Es braucht dringend eine Legitimationswirkung für **Responsible Disclosure**, beispielsweise indem klargestellt wird, dass Handlungen, die allein dem Aufdecken und Melden von Schwachstellen an die zuständigen Stellen dienen, straffrei sind. Diese Änderung müsste zwar im Strafrecht erfolgen, könnte aber im Zuge der NIS-2-Umsetzung angestoßen werden.

Fazit in diesem Punkt: Der Gesetzentwurf sollte um einen Abschnitt ergänzt werden, der einen **konsistenten Vulnerability-Disclosure-Prozess festlegt**. Alle dem BSI gemeldeten Lücken sind transparent an die Hersteller weiterzugeben. Eine Nutzung durch andere Behörden zu anderen Zwecken ist auszuschließen, solange kein besonderes Verfahren dafür gesetzlich vorgesehen ist. Diese Klarheit würde das Vertrauen der Bürger in die digitale Infrastruktur stärken und den Austausch mit der Security-Community verbessern. Gerade weil andere Staaten (und auch manche deutschen Sicherheitsbehörden) Schwachstellen als „Cyberwaffen” betrachten, muss das BSI wenigstens eine klare Sicherheitsorientierung zeigen. Es darf nicht der Eindruck entstehen, das BSI könne als Erfüllungsgehilfe für offensive Cyber-Operationen dienen. Die Umsetzung von NIS-2 bedeutet auch, eine Kultur der Sicherheit zu fördern – hierzu gehört zwingend der verantwortungsvolle Umgang mit Schwachstellen.

Harmonisierung mit weiterer Cyber-Sicherheitsgesetzgebung

Parallel zur NIS-2-Umsetzung arbeitet der Gesetzgeber an der Umsetzung der **CER-Richtlinie** (Critical Entities Resilience Act), die oft als KRITIS-Dachgesetz bezeichnet wird. Es ist essenziell, dass diese **Gesetzgebungsstränge gut verzahnt** werden. Der vorliegende Entwurf lässt allerdings eine erkennbare Abstimmung mit dem KRITIS-Dachgesetz vermissen. Dadurch drohen im schlimmsten Fall parallele, unkoordinierte Anforderungen an die Betroffenen. Unterschiedliche Definitionen, Schwellenwerte oder Prozesse würden für die Betreiber

- [5] D. Kunze in: Handbuch der Cyberkriminologie, Springer, 2023, DOI 10.1007/978-3-658-35439-8_22

kritischer Dienste einen erheblichen Mehraufwand und Rechtsunsicherheit verursachen. Um das zu vermeiden, sollte beispielsweise der Begriff der „besonders wichtigen Einrichtung“ (im NIS-2-Umsetzungsgesetz) mit dem der „kritischen Einrichtung“ (im KRITIS-Dachgesetz) konsistent sein. Idealerweise wird eine gemeinsame Verordnung erlassen, die einheitlich festlegt, welche Einrichtungen und Sektoren unter welche Kategorie fallen, anstatt dies in jedem Gesetz getrennt zu regeln. Auch die Schwellenwerte (z. B. ab welcher Größe ein Unternehmen als wesentlich gilt) sollten aufeinander abgestimmt sein.

Darüber hinaus ist eine **Angleichung der Terminologie** im Gesetz selbst wünschenswert. Die deutsche Umsetzung verwendet teils andere Begriffe als die Richtlinie, was verwirrend sein kann. Beispielsweise spricht die Richtlinie von „wesentlichen“ und „wichtigen“ Einrichtungen (essential and important entities). Der Entwurf nutzt hingegen „besonders wichtige“ und „wichtige“ Einrichtungen – ein scheinbar kleiner Unterschied, der jedoch die Rückkopplung zur EU-Ebene erschwert. Hier sollte man sich konsequent an den EU-Begriffen orientieren, um Missverständnisse zu vermeiden. Gleiches gilt für Begriffe wie Cybersicherheit, IT-Sicherheit, Netz- und Informationssicherheit usw., die oft synonym verwendet werden. Eine klare Definition im Gesetz würde ein gemeinsames Verständnis fördern.

Kurzum: Das NIS2UmsuCG darf nicht isoliert betrachtet werden. Es muss als **Teil eines Gesamtkonzepts** betrachtet werden, zu dem auch das KRITIS-Dachgesetz, das neue Bundesdigitalgesetz und andere Sicherheitsgesetze gehören. Eine übergreifende Abstimmung ist dringend nötig.

Schlussbemerkung und Fazit

Die vorstehenden Ausführungen machen deutlich, dass der Regierungsentwurf zwar ein wichtiger Meilenstein ist, in einigen Bereichen jedoch nachgeschärft werden muss. Deutschland hat derzeit eine fragmentierte Landschaft in der Cybersicherheit: Verschiedene Sektoren und Verwaltungsebenen sind unterschiedlich geschützt, Zuständigkeiten sind zersplittert und es fehlt mitunter an einer kohärenten Strategie. Diese Fragmentierung schwächt die gesamtstaatliche Resilienz. Das NIS2UmsuCG bietet die Chance, zumindest regulatorisch für mehr Einheitlichkeit zu sorgen – diese Chance sollte genutzt werden.

Zusammengefasst möchte ich die wichtigsten Empfehlungen betonen:

- **Kommunen einbeziehen:** Die Auslassung der Kommunalverwaltungen ist sachlich nicht begründbar und gefährdet die Cybersicherheit des Staates als Ganzes. Eine Einbeziehung schafft bundeseinheitliche Mindeststandards, schließt gefährliche Lücken und sorgt für einen gleichwertigen Schutz der Bürgerdaten überall im Land. Die Umsetzung muss von Bund und Ländern gemeinsam gestemmt werden – ggf. mit finanzieller Unterstützung –, aber sie ist unabdingbar.
- **Bundesverwaltung stärken:** Alle Bundesbehörden müssen denselben hohen Sicherheitsanforderungen genügen. Die derzeit vorgesehene Zweiklassengesellschaft (Ministerien vs. übrige Behörden) sowie die weitreichenden Ausnahmemöglichkeiten

unterminieren das Ziel der Richtlinie. Hier sollte der Innenausschuss Korrekturen vornehmen, um ein konsistentes Schutzniveau sicherzustellen – inklusive klarer Verantwortlichkeiten und Kontrollen.

- **BSI und CISO Bund befähigen:** Die zentrale Rolle des BSI muss mit ausreichender Unabhängigkeit, Ressourcen und Pflichten unterlegt werden, damit es seine Aufgaben effektiv wahrnehmen kann. Ein starker CISO Bund sollte die Cybersicherheit des Bundes koordinieren und vorantreiben. Ohne klare Führung und Kompetenzbündelung bleibt die Bundesverwaltung verwundbar.
- **Meldewesen und Schwachstellenmanagement verbessern:** Bürokratieabbau und Sicherheit gehen Hand in Hand, wenn Meldeströme gebündelt werden und alle Beteiligten von den Informationen profitieren. Ebenso muss der Umgang mit Sicherheitslücken gesetzlich so geregelt werden, dass Sicherheit stets Vorrang hat und Forschungsbeiträge willkommen sind. Hier besteht Nachholbedarf im Entwurf.
- **Ganzheitlichkeit gewährleisten:** Der Gesetzgeber sollte schließlich auf Widerspruchsfreiheit mit anderen Normen (KRITIS, DSGVO etc.) achten und die vorhandenen Instrumente konsistent einsetzen. Cyber-Sicherheit ist kein isoliertes Themenfeld, sondern berührt Verwaltungsmodernisierung, Datenschutz, Wirtschaftsschutz und nicht zuletzt die nationale Sicherheit. All diese Aspekte müssen berücksichtigt werden.

Die vorliegende Gesetzesinitiative kommt nach langer Vorbereitung zu einem entscheidenden Zeitpunkt. Die Bedrohungslage ist so hoch wie nie und die Bereitschaft, in Cybersicherheit zu investieren, wächst endlich an (auch dank EU-Vorgaben). **Es liegt nun am Parlament, den Entwurf so zu optimieren, dass er sein volles Potenzial entfaltet.** Die hier aufgezeigten Maßnahmen würden den Gesetzentwurf nicht grundlegend verändern, seine Wirkung jedoch erheblich verstärken. Sie sorgen dafür, dass Deutschland nicht nur das Mindestmaß der EU-Vorgaben erfüllt, sondern aktiv seine Cyber-Resilienz erhöht. Die Kosten dafür sind erheblich, doch ohne diese Maßnahmen wären die Kosten um ein Vielfaches höher, wie zahlreiche Vorfälle bereits bewiesen haben.

Abschließend möchte ich betonen: Nie war die Zeit günstiger als jetzt, um in die Cybersicherheit zu investieren. Der politische Wille ist vorhanden und die Notwendigkeit unbestritten. Nutzen wir also die Gelegenheit, mit dem NIS2-Umsetzungs- und Cybersicherheitsstärkungsgesetz einen großen Schritt nach vorn zu machen – für eine sicherere digitale Zukunft unseres Landes.

Sabine Griebsch

Managing Director GovThings / Cyber- und IT-Krisenmanagerin