21. Wahlperiode

Deutscher Bundestag
Innenausschuss

**Ausschussdrucksache 21(4)062 G**
vom 16. Oktober 2025

# Schriftliche Stellungnahme

von Prof. Timo Kob, HISOLUTIONS vom 15. Oktober 2025

Öffentliche Anhörung

Gesetzentwurf der Bundesregierung

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

**BT-Drucksache 21/1501**

# Stellungnahme zum Gesetzentwurf zur Umsetzung der NIS2-Richtlinie

von Prof. Timo Kob

## 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, wenn das Gesetz wie geplant auch zusätzliche Aspekte über die NIS2-Umsetzung hinaus aufnimmt.

Diese sind thematisch wünschenswert und inhaltlich in meinen Augen richtig, können aber durch notwendige Diskussionen, Betroffenenbeteiligungen etc. das Gesamtvorhaben verzögern. Ich werde dazu aber später auch noch im Detail eingehen.

Ich würde hier auch gar nicht die potenziellen Strafzahlungen durch die EU in den Vordergrund schieben, sondern einen ganz anderen Effekt:

Lt. Bitkom-Studie beträgt der jährliche Schaden durch Cyberattacken 200 Miliarden Euro pro Jahr.

Wenn das Gesetz also dazu beiträgt, diese Summe auch nur um 1% zu senken (oder alternativ den seit Jahren ungebrochenen Wachstumstrend entsprechend bremst oder bricht) reduziert dies den volkswirtschaftlichen Schaden um 2 Milliarden Euro und die daraus resultierenden Steuermehreinnahmen decken die vermeintlich zu hohen Kosten für staatliche Institutionen für einen ausreichenden Schutz mehrfach!

Leider warten aber Unternehmen wider aller Vernunft auf die Verabschiedung des Gesetzes, obwohl das, was fachlich gefordert wird, nicht nur heute klar ist, sondern auch aus purem Eigeninteresse sofort gemacht werden sollte (und zwar unabhängig, ob das Unternehmen reguliert werden soll oder nicht). Allein um diese mentale Blockade zu lösen, ist jeder Tag, den das EIGENTLICHE NIS2-Gesetz früher in Kraft tritt, ein gewonnener Tag.

## 2. Konkrete Kritikpunkte am Gesetzesentwurf

### 2.1. Nicht akzeptable Reduktionen auf staatlicher Seite

Die Angriffe auf Unternehmen und staatliche Institutionen nimmt seit Jahren zu. Die geopolitische Lage spiegelt sich auch im Cyberspace wieder. Auf diese steigende Bedrohungslage mit einer ABSENKUNG der Sicherheitsanforderungen zu reagieren, ist offensichtlich absurd.
Schon die Tatsache, dass Kommunen ausgenommen werden, ist eigentlich nicht hinnehmbar, dass dies nun aber auch noch für nachgeordnete Bundesbehörden gelten soll (§29) und zusätzlich sogar noch die seit Jahren verpflichtende (aber nur in geringem Maße erfüllte) Umsetzung des IT-Grundschutzes für diese gestrichen werden soll, muss zwingend zurückgenommen werden.

Neben dieser offensichtlichen Unlogik ergeben sich aber noch weitere Fragestellungen und Sollbruchstellen. Wie soll in Zukunft die Kommunikation zwischen den Behörden (Stichwort Netze des Bundes) funktionieren, wenn unterschiedliche Sicherheitsvorgaben gelten?

> *Wir schützen die Vordertür mit Stahlriegel und die Hintertür mit Flatterband. Welchen Weg wird der Einbrecher wählen?*

In dieser Logik könnte man dann gleich die Schutzmaßnahmen für alle senken, da es das Gesamtsicherheitsniveau auch nicht mehr absenkt. Oder schützen sich dann die Ministerien für ihren eigenen nachgeordneten Behörden?

Um die ganze Absurdität aufzuzeigen: Unternehmen, die z.B. nachgeordnete Behörden im Bereich Sicherheit beraten, müssen sich nach Grundschutz zertifizieren lassen, um Zugang zu Dokumenten mit der Einstufung VS-NFD zu erhalten, die Behörden brauchen aber weniger Schutzmaßnahmen, um VS oder Geheim zu verarbeiten.

> *Nachgeordnet heißt NICHT von nachrangigem Interesse für Angreifer!*

Wir haben im letzten Jahr den Sicherheitsvorfall auf das Bundesamt für Kartographie und Geodäsie erlebt, der auf einen chinesischer Cyberangriff zurückgeführt wurde. Hier bestand Zugriff auf sensible Daten von kritischen Infrastrukturen. Ist es unser staatlicher Ansatz, die derzeit beobachteten Drohnenflüge zur Ausspionierung kritischer Infrastrukturen dadurch zu reduzieren, in dem wir die gewünschten Daten interessierten Feinden barrierearm im Netz anbieten?

Ich möchte aber auch noch einen zweiten Aspekt aufzeigen: Im Gegensatz zum Zeitpunkt der ersten Anhörung haben wir jetzt ein Digitalisierungsministerium, auf dessen Erfolg wir alle unsere Hoffnungen setzen. Was wäre aber, wenn dieser Erfolg eintritt?

Wenn wir hier wirklich gut vorankommen und gleichzeitig bei der Sicherheit stehenbleiben oder gar zurückfallen, ist offenkundig, was passieren wird.

Die Tatsache, dass es in der Summe auf Bundesebene recht wenig (zumindest bemerkte) Vorfälle gab, liegt auch und gerade daran, dass wir so rückständig in der Digitalisierung waren und noch sind.

*Wenn ich mein rostiges Klapprad bisher nur mit einem Bindfaden festbinde und es trotzdem nicht gestohlen wurde, habe ich Glück gehabt.*
*Ich sollte das Experiment aber nicht mit einem neuen Rennrad wiederholen und erst recht nicht sogar auf den Bindfaden verzichten.*

Es ist also sogar ein doppelter Trend, der ein Mehr und nicht ein Weniger an Sicherheit verlangt: Steigende Bedrohung UND steigende Angriffsfläche durch höheren Digitalisierungsgrad.

Jede Einsparung an Sicherheit ist so de facto auch eine Durchkreuzen der Digitalisierungspläne, weil diese entweder unsicher betrieben werden oder der nötige Schutz dann in den Projekten finanziert und zeitaufwändig umgesetzt werden müssen.
Im letzten Fall ist die vermeintliche Kosteneinsparung durch Senkung der Anforderungen pure Augenwischerei.
Erst recht, wenn man auch die direkten und indirekten Kosten für die hierdurch geradezu zwangsläufig auftretenden zusätzlichen Vorfälle einkalkuliert. Nur, weil man sie nicht im Haushalt einplanen kann und muss, heißt es ja nicht, dass sie nicht entstehen.

Ergänzend möchte ich darauf hinweisen, dass die Kostenargumente, die zu dieser absurden Entscheidung führten, vorgeschoben sind. Ein Großteil der Kosten würden nicht auftreten, wenn man seine Hausaufgaben pflichtgemäß erfüllt hätte. Diese nun der NIS2 „in die Schuhe zu schieben“ ist unredlich.

Seit 8 Jahren besteht die Verpflichtung, den Grundschutz in den Behörden des Bundes umzusetzen. Seit 7 Jahren soll ein einheitliches Grundschutztool im Rahmen der „IT-Konsolidierung Bund“ ausgerollt werden. Der Umsetzungsgrad bis heute ist in beiden Fällen erschütternd schlecht.

Die hohen Aufwandsschätzungen liegen also vor allem daran, dass man bisher die Hausaufgaben nicht gemacht hat. Hinzu kommt, dass gefühlt jede Behörde jedes Rad neu erfindet.

*Claudia Plattner redet vom Ziel der „Cybernation“, aber selbst innerhalb der Bundesverwaltung sind wir noch nicht einmal ein „Cyber-Zollverein“.*

Die Aufwandsschätzungen basieren auf einem „Weiter so“ und nicht auf dringend nötigen neuen, kooperativen, digitalen Ansätzen. Dieser Konstruktionsfehler führt zu unnötigen Aufwänden.

Wir lassen uns von vermeintlichen Kosten ineffizienter Ansätze abschrecken und wollen die Anforderungen absenken, anstatt die Gelegenheit zu nutzen, nicht nur die Rolle eines Bundes-CISOs zu schaffen, sondern dies auch mit der konkreten Maßgabe und Befugnis zu versehen, aus 200 Teilprojekten eine Gemeinschaftsaufgabe zu machen, Doppelarbeiten zu verhindern, Best Practices zu multiplizieren etc.

Dazu gehört die Modernisierung des IT-Grundschutzes, wie es das BSI ja gerade durchführt, die flächendeckende verpflichtende Umsetzung der Konsolidierungsmaßnahme „Einheitliches Grundschutz-Tool“ um z.B. Doppelarbeiten zu reduzieren, Prozesse zu verkürzen (und als kostenlosen „Beifang“ sogar noch einen Beitrag zu einem Lagebild zu liefern), und eben ein Bundes-CISOs, der nicht nur die Zielerreichung überwacht, sondern auch mit wirklicher Weisungsbefugnis auseinanderstrebende Projekte zusammenhält.

## 2.2. Aufgaben und Besetzung der Rolle „CISO Bund“

Um die zuvor geforderten Veränderungen umzusetzen, muss der CISO Bund kraftvoller und operativer etabliert werden, als die aktuell maximal unscharfe Definition. So vage, wie in §48 das Amt des Koordinators für Informationssicherheit definiert ist, droht es zu einem zahnlosen Tiger und reiner Symbolpolitik zu verkommen.

Erforderlich ist hier aus fachlicher Sicht eine klare Weisungsbefugnis, um die derzeit leider oft als Freifahrtschein zur Nichtbeachtung genutzte Ressortunabhängigkeit auszuhebeln.

> *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.

Verschiedene Seiten haben ihr Interesse an der Rolle bekundet. BMDS, BMI, BSI, selbst eine Anbindung an das Kanzleramt wurde vorgeschlagen.

Jede der Ansätze hat ihre Vor- und Nachteile. Das BSI allein hätte Durchsetzungsschwierigkeiten, eine Anbindung an eines der Ministerien krankt (egal in welcher Variante) an der Aufteilung der bisherigen Abteilung CI auf zwei Ministerien, es sind aber (richtigerweise) auch nicht alle operative relevanten Kompetenzen in den Häusern vorhanden, die zumindest für die von mir ausgeprägte Aufgabenbeschreibung benötigt. Daher geht meine Empfehlung – zugegebenermaßen durchaus mit leichten Störgefühlen – in Richtung BSI. Eine optimale Lösung sehe ich nicht, eine Variante mit dem BSI scheint mir aber die geringsten, respektive die am leichtesten ausgleichbaren, Nachteile zu besitzen.

Dem BSI diese Aufgabe ohne sonstige Anbindung zu übergeben, würde das Problem aber nicht beheben, da dies nur zu einer Verlängerung des jetzigen Zustands in die Zukunft führen würde: dem wissentlichen Ignorieren der Vorgaben. Dies haben wir mit dem UP Bund leidvoll erfahren. Es braucht also einer direkten Ein- und Anbindung eines Ministers (ich halte selbst die Rolle eines Staatssekretärs hier für zu niedrig), um Konflikte und Blockaden schlimmstenfalls bis an den Kabinettstisch oder den zukünftigen Nationalen Sicherheitsrat zu bringen (wenn man hier nicht sogar dem/der CISO Bund direkt einen Platz einräumt).

Die Verbindung der Position mit der der Schaffung eines explizit nur hierfür zuständigen zweiten Vize-Präsidenten des BSI, wie es andere Sachverständige in der Anhörung vorschlugen, ist eine zumindest überdenkenswerte Option.

## 2.3. Eingeschränkte Detektionsmöglichkeiten

Leider wird hier bei der in §15 definierten Möglichkeit zur Detektion von Angriffsmethoden und von Sicherheitsrisiken immer noch nur der halbe Schritt getan, in dem dies auf die von NIS2 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 nichts mit dem Ausnutzen von Schwachstellen zu tun. Claudia Plattner beschrieb das plastisch 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.

Wenn selbst ein gewiss nicht der übermäßigen Forderung nach mehr Überwachungsbefugnissen verdächtiger Verein wie die AG KRITIS dies in ihrer Stellungnahme verlangt, scheint es hier gesellschaftlich einen breiten Konsens zu geben, so dass diese etwas ängstlich wirkende Beschränkung nicht nachvollziehbar ist

## 2.4. Vernachlässigbare Geschäftsbereiche

Der hinter dieser Regelung stehende Gedanke ist grundsätzlich positiv.

Leider ist er aber so vage formuliert, dass er aktuell mehr zur Verunsicherung denn zu angemessenem Handeln führt.
Hier bedarf es einer klaren Definition, bis wann etwas als vernachlässigbar angesehen werden kann.
Es spielt auch die Frage der Kritikalität eine Rolle, es kann sich also nicht nur etwa auch Anteil am Geschäftsvolumen als Kriterium handeln.
Als Nicht-Jurist enthalte ich mich einer Bewertung, inwieweit eine solche Regelung zu einem Verstoß gegen die europäischen Vorgaben führt, da es diesen Passus auf europäischer Ebene nicht gibt.

Als Praktiker würde ich aber argumentieren, dass alle Länder außer Deutschland hier im Zweifelsfall auch ohne spezifische Regelung in diesem Sinne agieren werden. Dies zeigt u.a. die nationale Interpretation der DSGVO, die auch in allen Mitgliedsländern gilt, aber gefühlt nur in Deutschland zu Problemen führt, weil es leider in unserem Lande an der Fähigkeit zu angemessen-pragmatischen Auslegung von Regelungen zu fehlen scheint.

## 2.5. Kritische Komponenten

Das Thema ist wichtig und die Ansätze sind richtig. Wir müssen hier zwingend agieren und zwar nicht nur in der Telekommunikation (Stichwort Wechselrichter). Ich rate aber dazu, dies aus der NIS2-Umsetzung zu entfernen und zeitnah anderweitig zu regeln.
Das Thema ist kompliziert, die Interessenlage der deutschen Wirtschaft differenziert und es sollte, wie schon in der Einleitung geschrieben, keinerlei weitere Verzögerungen für die NIS2-Umsetzung geben, die mir hier aber bei der wünschenswerten und nötigen Einbindung aller Betroffenen unvermeidbar erscheint.

## 2.6. 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 technischen und baulichen Infrastrukturen 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.

> *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.

Diesen Punkt möchte ich aber NICHT in der aktuellen Umsetzung der europäischen NIS2-Vorgaben berücksichtigt sehen, sondern zeitnah im Nachgang geklärt wissen.

# 3. Zur Person

Prof. Timo Kob ist Gründer und Vorstand der HiSolutions AG, einem Beratungshaus für Cybersecurity und Digitalisierung mit rund 400 Mitarbeitern.

Er verfügt über umfangreiche Erfahrungen aus Projekten des Bundes, der Länder und Kommunen, ist BSI-akkreditierter IT-Grundschutzauditor, Professor für Cybersecurity und Wirtschaftsschutz an der Hochschule Campus Wien sowie Vorsitzender respektive Vorstandsmitglied verschiedener Fachkommissionen im Wirtschaftsrat, Bitkom und BDI.