21. Wahlperiode

Deutscher Bundestag
Innenausschuss

Wortprotokoll der 11. Sitzung

Innenausschuss
Berlin, den 13. Oktober 2025, 15:00 Uhr
Konrad-Adenauer-Str. 1, 10557 Berlin
Paul-Löbe-Haus, Raum 4 600

Vorsitz: Josef Oster, MdB

Tagesordnung - Öffentliche Anhörung

Tagesordnungspunkt 1 **Seite 4**

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

Federführend:
Innenausschuss

Mitberatend:
Ausschuss für Digitales und Staatsmodernisierung
Haushaltsausschuss (mb und § 96 GO)

Berichterstatter/in:
Abg. Marc Henrichmann [CDU/CSU]
Abg. Steffen Janich [AfD]
Abg. Johannes Schätzl [SPD]
Abg. Dr. Konstantin von Notz [BÜNDNIS 90/DIE GRÜNEN]
Abg. Jan Köstering [Die Linke]

Anwesende Mitglieder des Ausschusses

Fraktion	Ordentliche Mitglieder	Stellvertretende Mitglieder
CDU/CSU	Gregosz, David Hain, Heiko Henrichmann, Marc Oster, Josef Schmidt, Sebastian Seif, Detlef Silberhorn, Thomas	
AfD	Janich, Steffen Raue, Arne	
SPD	Baldy, Daniel Fiedler, Sebastian	Bettermann, Daniel
BÜNDNIS 90/ DIE GRÜNEN	Dillschneider, Jeanne Notz, Dr. Konstantin von	
Die Linke	Köstering, Jan Vogtschmidt, Donata	

Liste der Sachverständigen
Öffentliche Anhörung am Montag, 13. Oktober 2025, 15.00 Uhr
„NIS-2-Richtlinien-Umsetzungsgesetz“

Stand: 8. Oktober 2025

Ferdinand Gehringer[1)]
Konrad-Adenauer-Stiftung e.V., Berlin
Abteilung Internationale Politik und Sicherheit

Sabine Griebsch[4)]
Management Director bei GovThings

Dr. Sven Herpig[2)]
interface
Leiter Cybersecurity Policy and Resilience

Prof. Dr. Dennis-Kenji Kipker[3)]
Universität Bremen
cyberintelligence.institute, Frankfurt am Main

Prof. Timo Kob[1)]
HiSolutions AG, Berlin

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

Prof. Dr. Meinhard Schröder[2)]
Universität Passau
Lehrstuhl für Öffentliches Recht, Europarecht und Informationstechnologierecht

---

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

Die Stellungnahmen zur Anhörung sind auf der Internetseite des Ausschusses abrufbar.

Beginn der Sitzung: 15.02 Uhr

Tagesordnungspunkt 1

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

Amt. Vors. **Josef Oster** (CDU/CSU): Verehrte Kolleginnen und Kollegen, es ist 15.00 Uhr. Wir wollen keine Zeit vergeuden und mit unserer Anhörung heute Nachmittag beginnen. Es ist ein weltpolitisch ereignisreicher Tag. Das soll uns aber nicht davon abhalten, hier im Innenausschuss solide und gute Sacharbeit zu machen. Ich darf daher die 11. Sitzung des Innenausschusses eröffnen, darf Sie alle sehr herzlich begrüßen, auch für diejenigen, die uns an den Bildschirmen zusehen. Mein Name ist Josef Oster. Ich bin der amtierende Vorsitzende des Innenausschusses und darf diese Anhörung der Sachverständigen heute leiten. Thema ist der Gesetzentwurf der Bundesregierung zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung auf der Bundestagsdrucksache 21/1501. Vorweg danke ich schon den Sachverständigen ganz herzlich, dass sie unserer Einladung nachgekommen sind und uns heute hier mit ihrer Expertise zur Verfügung stehen und dann später auch die Fragen der Kolleginnen und Kollegen beantworten werden und uns mitunter schon im Vorfeld ihre schriftlichen Stellungnahmen zur Verfügung gestellt haben.

Ich begrüße die von den Fraktionen benannten hier anwesenden Sachverständigen in alphabetischer Reihenfolge: Das sind Herr Ferdinand Gehringer, Sabine Griebsch, Professor Dr. Dennis-Kenji Kipker, Professor Timo Kob, Felix Kuhlenkamp und Professor Dr. Meinhard Schröder. Das sind die Sachverständigen, die hier im Saal anwesend sind. Zugeschaltet per Videokonferenz ist uns der Sachverständige Dr. Sven Herpig. Für das Bundesministerium des Innern darf ich den Leiter des Grundsatzreferates Cybersicherheit, Dr. Daniel Meltzian, hier herzlich begrüßen.

Die Sitzung wird live im Bundestagsfernsehen und auch auf der Homepage des Deutschen Bundestages übertragen und ab morgen auch in der Mediathek zum Abruf bereitgestellt werden. Ich darf mich für die schriftlich zugegangenen Stellungnahmen bei den Sachverständigen sehr herzlich bedanken. Sie sind den Ausschussmitgliedern zugänglich gemacht worden. Ich darf darauf hinweisen, dass von der heutigen Anhörung ein Wortprotokoll erstellt wird, das Sie anschließend auch zur Korrektur erhalten werden. Wir haben ein Zeitfenster bis 17.00 Uhr vorgesehen und in der geübten Praxis werden wir das so durchführen, dass die Sachverständigen zunächst die Möglichkeit erhalten, ein Eingangsstatement mit einer maximalen Dauer von drei Minuten abzugeben und dann steigen wir in die Fragerunden der Fraktionen ein. Dazu werde ich nachher noch etwas sagen. Und wir starten das Ganze in alphabetischer Reihenfolge, ich darf zunächst Herrn Gehringer um sein Eingangsstatement bitten. Bitte schön.

SV **Ferdinand Gehringer** (Konrad-Adenauer-Stiftung): Vielen Dank, sehr geehrter Herr Vorsitzender, sehr geehrte Abgeordnete, sehr geehrte Mitarbeiter der Abgeordneten, liebes Publikum auf der Tribüne. Ich freue mich, dass ich heute Nachmittag ein paar Einschätzungen zum aktuellen Gesetzentwurf abgeben darf und werde mich zunächst auf fünf zentrale Punkte beschränken.

Erstens: Schnelles und einheitliches Handeln. Die NIS-2-Richtlinie und die CER-Richtlinie müssen harmonisiert und zügig umgesetzt werden. Gesamtstaatliche Resilienz muss ganzheitlich, ganz nach dem „Allgefahrenansatz“ verinnerlicht werden. Doch die uneinheitliche Umsetzung, die wir derzeit in Deutschland erleben, schwächt unsere Resilienz, erhöht den Aufwand für Unternehmen und untergräbt die Akzeptanz. Deshalb brauchen wir einheitliche Begriffe, Meldewege und die Erstellung eines gemeinsamen Lagebildes. Eine weitere Verzögerung von NIS-2 und der CER-Richtlinie und damit dem KRITIS-Dachgesetz sind weder nachvollziehbar noch vertretbar!

Zweitens: Erfordernis berücksichtigen. Die gesamte Bundesverwaltung muss in die NIS-2-Richtlinie einbezogen werden. Ausnahmen bei der Bundesverwaltung sind nicht mehr vertretbar. Finanzielle oder organisatorische Einwände greifen zu kurz. Cybersicherheit ist eine dauerhafte staatliche

Aufgabe und durch die Ausnahme von der Schuldenbremse finanziell ebenfalls gedeckt. Die bisherige Regelung schwächt die Gesamt-Resilienz und sendet ein falsches Signal an die Wirtschaft, an die Gesellschaft und vor allen Dingen auch an andere Verwaltungen der Kommunal- und der Landesebene. Deshalb sollte die gesamte Bundesverwaltung denselben Sicherheitsanforderungen unterliegen, um ein einheitlich hohes Schutzniveau zu gewährleisten. Viele Behörden nutzen gemeinsame Strukturen, weshalb ein umfassender Schutz notwendig ist. Das Gleiche gilt für Staat und Regierung, dass sie auch im Ernstfall funktionsfähig und demnach robust und cybersicher sind.

Drittens: Chance nutzen. Das Information-Sharing-Portal muss zum zentralen Knotenpunkt werden. Angesichts vernetzter Lieferketten und Supply-Chain-Angriffe reicht es nicht mehr aus, nur regulierte Betriebe zu schützen. Da braucht es Anreize für kleine und mittelständische Unternehmen, die nicht von der NIS-2 umfasst sind, Vorfälle zu melden und Sicherheits- und Resilienz-Maßnahmen umzusetzen. Das Information-Sharing-Portal, im Gesetzesentwurf als „Plattform“ bezeichnet, sollte Echtzeitinformation, ein Cyber-Lage-Dashboard und zielgruppengerechte Handlungsempfehlungen sowie regionalspezifische Unterstützungsangebote, Kontaktdaten von Meldebehörden und Erste-Hilfe-Maßnahmen bieten – bidirektional, vernetzt und praxisnah. Dies bietet Motivation für freiwillige Meldungen und Teilhabe an mehr Cybersicherheit.

Viertens: Sicherheit austarieren und Vertrauen aufbauen. Wir brauchen klare Regeln für kritische Komponenten, transparent, flexibel und bürokratiearm. Die Untersagung unsicher Komponenten muss auf klaren objektiven Kriterien basieren.

Fünftens: Fachlichkeit stärken. Der Bundes-CISO (Chief Information Security Officer) braucht klare Kompetenzen und eine starke Verortung. Klar definierte Aufgaben, Durchsetzungsbefugnisse und Ressourcen sind essenziell. Im Übrigen verweise ich auf meine schriftliche Stellungnahme und danke zunächst für die Aufmerksamkeit.

Amt. Vors. **Josef Oster** (CDU/CSU): Vielen Dank, Herr Gehringer. Es geht weiter mit Frau Griebsch, bitte.

SVe **Sabine Griebsch** (GovThings): Sehr geehrte Ausschussmitglieder, sehr geehrte Damen und Herren, vielen Dank für die Gelegenheit zur nationalen Umsetzung der NIS-2-Richtlinie Stellung nehmen zu dürfen. Ich blicke inzwischen auf mehr als 20 Jahre Erfahrung auf kommunaler und auf Landesebene zurück. Ich war Chief Digital Officer und bin inzwischen Cyber- und IT-Krisenmanagerin. Ich habe Kommunen digitalisiert. Nun sehe ich regelmäßig, wie ihre Infrastrukturen für die Digitalisierung innerhalb von Minuten von Angreifern verschlüsselt werden. Inzwischen bin ich mit Themen im Bereich der Gesamtverteidigung befasst, was meinen Blick auf die Lage im Inneren und nach außen weiter schärft.

Vor diesem Hintergrund möchte ich ausdrücklich den Fokus auf die Einbeziehung der Kommunen in den Gesetzentwurf legen. Aus fachlicher Sicht und in Anbetracht der aktuellen Sicherheitslage besteht hier eine kritische Lücke! Kommunen erbringen wesentliche Leistungen der Daseinsvorsorge. Angesichts weiter steigender Angriffszahlen und immer komplexerer Bedrohung brauchen wir einen koordinierten Ansatz mit einheitlicher Abwehrstrategie, gemeinsam Lagebildern und abgestimmten Mindeststandards auf allen Verwaltungsebenen, um einen geschlossenen Schutzschild gegen Cyberangriffe aufzubauen. Die Richtlinien bieten den Mitgliedstaaten ausdrücklich die Option, lokale Verwaltungen in den Anwendungsbereich aufzunehmen. Die Entscheidung der Bundesregierung, die Absicherung der kommunalen IT vorerst den Ländern zu überlassen, belässt faktisch einen großen Teil der staatlichen IT verwundbar und verfestigt die bestehenden Fragmentierungen der Sicherheitsarchitektur. Sie alle wissen: die Kommunen sind an den Netzen der Länder und an den Netzen des Bundes angeschlossen. Rechtlich ist die Ausweitung auf die Kommunen zulässig. Ein Gutachten des Wissenschaftlichen Dienstes des Bundestages hat dies auch klargestellt. Einzelheiten zur Möglichkeit der Umsetzung von Rahmenvorgaben durch den Bund zur Finanzierbarkeit und Umsetzbarkeit finden sich in der schriftlichen Stellungnahme. Die Sachlage spricht klar für eine Einbeziehung der Kommunalverwaltung in den Geltungsbereich des NIS-2-Umsetzungsgesetzes.

Gleiche Sicherheitsstandards müssen für alle Behörden gelten, für alle Bundesbehörden gelten. Der Entwurf sieht höhere Auflagen für Ministerien als für nachgeordnete Behörden vor – diese Zweiteilung lässt sich kaum rechtfertigen. Bundes-

behörden sollten vergleichbar hohe Sicherheitsmaßnahmen umsetzen, andernfalls werden die weniger geschützten Stellen zum Einfallstor für Angreifer, die sich das schwächste Glied suchen. Wir haben hier wieder den Vergleich zu den Verwaltungen in der vernetzten Infrastruktur.

Die Stärkung des BSI und des CISO Bund ist notwendig. Das Bundesamt für Sicherheit in der Informationstechnik muss gestärkt und unabhängiger aufgestellt werden. NIS-2 verlangt ausdrücklich, dass zuständige Stellen frei von unzulässiger Einflussnahme agieren können – untersteht das BSI weiterhin dem Innenministerium, ist dies eventuell nicht gegeben. Im Entwurf fehlen dazu klare Regelungen. Das BSI muss weitestgehend weisungsfrei agieren können.

Meldewesen und Schwachstellenmanagement: Die Meldepflichten müssen praxisnah und effizient sein, Sicherheitsvorfälle sollten gebündelt werden, damit nicht mehrfach an verschiedenen Stellen berichtet werden muss. Auch für Kommunen muss der Zugang zum Lagebild über alle Ebenen hinweg gegeben sein. Genauso konsequent muss der Umgang mit Schwachstellen geregelt werden. Entdeckte Sicherheitslücken sind umgehend zu schließen und an den Hersteller weiterzugeben! Weisungen, die dem entgegenlaufen, dürfen keine Rolle spielen. Außerdem brauchen wir eine Kultur des Responsible Disclosure – wer Schwachstellen meldet, darf nicht dafür bestraft werden!

Die Bedrohungslage war noch nie so gravierend. Doch gleichzeitig wächst die Bereitschaft, in Sicherheit zu investieren. Das Parlament sollte die Gelegenheit nutzen, den Entwurf nachzuschärfen, damit er sein volles Potenzial entfalten kann.

Amt. Vors. **Josef Oster** (CDU/CSU): Vielen Dank, Frau Griebsch. Also ich kann Ihnen sagen, wir haben selten Sachverständige, die in drei Minuten so viel hineinpacken, wie Ihnen das jetzt gelungen ist. Vielen Dank dafür. Wir fahren fort mit dem zugeschalteten Sachverständigen Dr. Herpig. Herr Herpig, bitte.

SV **Dr. Sven Herpig** (interface): Sehr geehrter Herr Vorsitzender, sehr geehrte Ausschussmitglieder, Abgeordnete und Mitarbeitende, die mit beiden Beinen fest auf dem Boden unserer freiheitlich-demokratischen Grundordnung stehen, sehr geehrte interessierte Öffentlichkeit! Unabhängig davon, welchen Lagebericht zur IT-Sicherheit in Deutschland man heranzieht – alle kommen zum gleichen Ergebnis: Die Bedrohungslage ist hoch und nimmt weiter zu. Kriminelle, ausländische Nachrichtendienste und andere Bedrohungsakteure agieren zunehmend effizienter und effektiver. Auch die Gefährdungslage, also die konkrete Auswirkung dieser Bedrohung auf unsere IT-Infrastrukturen ist mehr als beunruhigend! Im geleakten Bericht des Bundesrechnungshofs zur IT-Sicherheit in der Bundesverwaltung heißt es unmissverständlich: „Die Informationstechnik des Bundes ist nicht bedarfsgerecht geschützt …“ Doch nicht nur die IT-Infrastrukturen der Bundesverwaltung sind problematisch, auch in zentralen Digitalisierungsprojekten wie der elektronischen Patientenakte haben SicherheitsforscherInnen teils gravierende Schwachstellen und Architekturfehler entdeckt.

Vor diesem Hintergrund überrascht es kaum, dass die Diskussion zur Umsetzung der NIS-2-Richtlinie seit Langem vor allem über den Anwendungsbereich geführt wird. Ein breiter Anwendungsbereich innerhalb der Bundesverwaltung ist jedoch nur dann sinnvoll, wenn die vorgesehenen Maßnahmen auch tatsächlich umgesetzt werden. Und um dies zu gewährleisten, zu überprüfen und bei Verfehlungen gegenzusteuern, braucht es eine starke, unabhängige und fachlich kompetente Instanz – die oder den Chief Information Security Officer des Bundes, kurz: CISO Bund. Damit diese Rolle wirksam zur Verbesserung der IT-Sicherheit Deutschlands beitragen kann, müssen mehrere Voraussetzungen erfüllt sein. Im Sinne eines Systems von Checks and Balances und auf Grundlage international anerkannter Best Practices muss die Funktion des CISO Bund oder der CISO Bund fachlich unabhängig vom Chief Information Officer-Bund, also dem CIO Bund, ausgestaltet werden. Der oder die CISO Bund sollte mit klaren Prüfbefugnissen, einer Koordinierungsfunktion zur Harmonisierung von IT-Sicherheitsstandards, einem Vortragsrecht bei Vorgesetzten des CIO Bund sowie einem regelmäßigen Berichtsrecht gegenüber dem Bundesrechnungshof und den zuständigen Parlamentsausschüssen ausgestattet werden. Zudem muss es sich bei dem oder der CISO Bund um eine eigenständige Position mit angemessener personeller und finanzieller Ausstattung handeln, nicht um eine zusätzliche Rolle einer bestehenden Leitungsperson, etwa der Präsidentin des Bundesamts für Sicherheit in der Informationstechnik. Denkbar wäre beispielsweise eine fachlich vom

BMI und vom BMDS unabhängige Vizepräsident-Innen-Position innerhalb des BSI. Sollte die Rolle des oder der CISO Bund dort verankert werden, sollte zudem § 1 BSIG angepasst werden, zum Beispiel in: „Seine Aufgaben führt das Bundesamt auf Grundlage wissenschaftlich technischer Erkenntnisse durch.“ Gerade bei einem erweiterten Anwendungsbereich ist es nicht nachvollziehbar, warum das BSI wissenschaftlich technisch nur gegenüber Bundesministerien agieren soll und nicht gegenüber anderen Bundesbehörden, den Länderverwaltungen, der Wirtschaft und der Gesellschaft insgesamt. Vielen Dank.

Amt. Vors. **Josef Oste**r (CDU/CSU): Vielen Dank, Herr Dr. Herpig. Wir fahren fort hier im Saal mit Herrn Professor Dr. Kipker. Bitte schön.

SV **Prof. Dr. Dennis-Kenji Kipker** (Universität Bremen): Sehr geehrter Herr Vorsitzender, sehr geehrte Ausschussmitglieder, sehr geehrte Damen und Herren. Vielen Dank erst einmal für die Möglichkeit hier heute Stellung nehmen zu können. Der Entwurf eines NIS-2-Umsetzungsgesetzes sieht seinem Zielbild nach für Deutschland die Schaffung eines einheitlich hohen Rechtsrahmens für die digitale Resilienz in unsicheren Zeiten vor, scheitert in der konkreten Realisierung jedoch, indem er uneinheitliche, fragmentierte Regelungen schafft, die die Informationssicherheit in Teilen zwar stärken, jedoch in der Fläche nach wie vor Raum für erhebliche Vulnerabilitäten und auch Rechtsunsicherheit lassen. Mit dem Ziel, die Cybersicherheit in Deutschland nachhaltig zu stärken und gegen aktuelle und zukünftige hybride Bedrohungen angemessen gerüstet zu sein, ist das nicht vereinbar. Im Folgenden möchte ich deshalb einige Schwerpunkte aus meiner schriftlichen Stellungnahme hervorheben.

Erstens: Zur Rolle des BSI. Obwohl die Fragen rund um die Verbesserung der Unabhängigkeit des BSI seit mehreren Jahren breit erörtert werden, sind keine nennenswerten Fortschritte ersichtlich. Die Empfehlungen aus der AG BSI, die unter der Vorgängerregelung erarbeitet wurden, finden im vorliegenden Entwurf der Bundesregierung keine Berücksichtigung, um eine sachlich und fachlich unabhängige Arbeit der Behörde zu gewährleisten.

Zweitens: Zum Schwachstellenmanagement. Nach wie vor fehlen klare Regelungen für ein staatliches Schwachstellenmanagement, wie mit gemeldeten Informationen umgegangen wird. Das BSI-Gesetz ist ein IT-Sicherheitsgesetz und kein Gesetz, das Möglichkeiten zur Kompromittierung von IT-Infrastruktur offenlässt. Hier wäre eine gesetzliche Klarstellung zur unverzüglichen Schließung von ermittelten Schwachstellen nicht nur wünschenswert, sondern eben auch dringend geboten.

Drittens: Resilienz der öffentlichen Verwaltung. Auch unter diesem Gesichtspunkt bleibt der vorgelegte Gesetzentwurf leider weit hinter den Erwartungen zurück und läuft dem Ziel der Bundesregierung, die digitale Resilienz auch in der Bundesverwaltung nachhaltig zu steigern, leider auch zuwider. Durch die unterschiedlichen Anforderungsniveaus in der Bundesverwaltung in Kombination mit zahllosen Ausnahmetatbeständen entsteht vielmehr eine Zweiklassengesellschaft der Informationssicherheit auf doppelte Weise: einmal im Verhältnis vom Bundeskanzleramt und Bundesministerien zu den übrigen Einrichtungen der Bundesverwaltung, sowie im Verhältnis Staat und Privatwirtschaft. Zu empfehlen ist im Ergebnis daher, den IT-Grundschutz für alle Einrichtungen der Bundesverwaltung verbindlich festzuschreiben. Sollte die Aufweichung durch Finanzierungsfragen begründet werden, wäre dies auch angesichts der zunehmenden Bedrohungslage gegen staatliche Einrichtungen, die bereits meine Vorredner skizziert haben, höchst kurzsichtig und in der Vorbildfunktion des Staates fatal.

Der letzte Punkt betrifft den CISO Bund: Der Aufbau eines Koordinators für Informationssicherheit ist auf jeden Fall begrüßenswert. Dennoch ist dessen Rolle auch im aktuellen Regierungsentwurf bis auf einen einzelnen Satz so weit entkernt, dass weder eine klare organisatorische Struktur, Befugnisse, noch eine Arbeitsweise erkennbar sind, sodass er mehr oder weniger nur noch ein Feigenblatt für die Informationssicherheit in der Bundesverwaltung darstellt. Ein CISO Bund wird nur dann effektiv arbeiten können und seiner Aufgabenbestimmung hinreichend gerecht, wenn er entsprechende Durchsetzungsbefugnisse erhält, sein Tätigkeitshorizont klar umschrieben ist und er hinreichend unabhängig im nationalen Verwaltungsgefüge angesiedelt wird und auch entsprechend agieren kann. Danke schön.

Amt. Vors. **Josef Oster** (CDU/CSU): Vielen Dank, Herr Kipker. Es geht weiter auf der anderen Seite. Herr Professor Kob, bitte.

SV **Prof. Timo Kob** (HiSolutions): Sehr geehrter Herr Vorsitzender, sehr geehrte Abgeordnete. Vielen Dank für die Möglichkeit, in dieser Anhörung Stellung nehmen zu dürfen. Auch wenn es definitiv mehrere Themen gibt, über die es zu diskutieren gilt, möchte ich mich in meinem Statement ob der Zeitlimitation auf einen Punkt konzentrieren: Die unsägliche Ausnahme der nachgeordneten Behörden. Ausnahme bedeutet nicht etwa Verzicht auf eine Erhöhung der Anforderungen, sondern es ist ein Absenken der Anforderungen. Statt die Cyber-Sicherheit zu stärken, schwächt das Gesetz sie also sogar. Seit 2017 sind die Ministerien und nachgeordneten Behörden durch den Umsetzungsplan Bund (UP Bund) verpflichtet, den IT-Grundschutz umzusetzen. Der Umsetzungsgrad nach acht Jahren ist erschütternd! Selbst wenn die Bedrohungslage seitdem nicht gestiegen wäre, die Tatsache, dass es in der Summe auf Bundesebene recht wenig, zumindest bekannt gewordene Vorfälle gab, liegt, wenn wir ehrlich sind, auch und gerade daran, dass wir so miserabel in der Digitalisierung waren. Boshaft gesagt: Solange ich Faxgeräte verwende, ist das Risiko halt niedriger!

Jetzt haben wir ein Digitalisierungsministerium, dem wir alle maximalen Erfolg wünschen. Wenn wir hier aber wirklich gut vorankommen und gleichzeitig bei der Sicherheit stehen bleiben oder zurückfallen, ist doch selbst einem Kind klar, was passieren wird. Es ist ein doppelter Trend, der ein Mehr und nicht ein Weniger an Sicherheit verlangt, steigende Bedrohungen *und* steigende Angriffsfläche durch hoffentlich massiv höheren Digitalisierungsgrad. Jede Einsparung an Sicherheit ist so de facto eine Sabotage an den Digitalisierungsplänen, weil diese entweder unsicher betrieben werden oder die nötigen Schutzmaßnahmen dann in den Projekten finanziert und zeitaufwendig umgesetzt werden müssen. Die Tatsache, dass die Kosten als Argument für die Absenkung der Anforderungen dienen, ist ehrlich gesagt abenteuerlich. Zum einen ignoriert man hier die Kosten für direkte Schäden und deren Behebung, die geradezu zwangsläufig auftreten werden, wenn man die Vorsorge nicht massiv stärkt. Vor allem aber, dass die meisten Kosten jetzt als untragbar angesehen und dem NIS-2-Umsetzungsgesetz zugeschrieben werden, ist Folge der Verfehlung der vorigen Jahre!

Da mein Unternehmen einerseits den Rahmenvertrag für die Sicherheitsberatung der Bundesverwaltung hält und andererseits sein Tochterunternehmen mit dem Informationstechnikzentrum Bund (ITZBund) die Maßnahme „Einheitliches IT-Grundschutztool“ aus dem Rahmen IT-Konsolidierung-Bund umsetzen soll, kann ich Ihnen einmal einen Innenblick geben. Beim Sicherheitsberatungsvertrag sind aktuell 35 Prozent der Zeit abgelaufen, beauftragt sind 21 Prozent, abgearbeitet sind 11 Prozent des Budgets. Der Drang, die unstrittig vorhandenen Sicherheitsdefizite zu beheben, ist also bis heute eher gering und die hohen Aufwandsschätzungen liegen also vor allem daran, dass man bisher die Hausaufgaben nicht gemacht hat. Sie liegen aber auch daran, dass gefühlt jede Behörde jedes Rad neu erfindet und das, obwohl man zu wenig Köpfe hat. Was mache ich, wenn ich zu wenig Köpfe habe? Ich digitalisiere und da kommen wir zur zweiten klaffenden Lücke der Tool-Unterstützung, wie sie eben die Konsolidierungsmaßnahmen seit 2018 anstreben. Auch hier ein Innenblick: Nach sieben Jahren nutzen von den rund 200 potenziell angedachten Behörden nur 25 Behörden das vom ITZBund angebotene einheitliche Tool. Circa 25 weitere Häuser nutzen das Tool als eigene Installation ohne ITZBund, können also auch nur den halben Nutzen ziehen, weil sie nicht auf gemeinsame Inhalte zugreifen können. Claudia Plattner redet vom Ziel der Cyber-Nation, aber selbst innerhalb der Bundesverwaltung sind wir noch nicht einmal ein Cyber-Zoll-Verein!

Bei der jetzigen Aufwandsschätzung wurde aber abgefragt, wie man denn mit alten Ansätzen zum Ziel kommt. Da liegt dann eben schon der Denkfehler. Sie kennen sicher das Bonmot von Einstein: Wahnsinn ist, immer wieder das Gleiche zu tun und andere Ergebnisse zu erwarten. Wir lassen uns von vermeintlichen Kosten ineffizienter Ansätze abschrecken und wollen die Anforderung absenken, anstatt die Gelegenheit zu nutzen, nicht nur die Rolle eines Bundes-CISOs zu schaffen, sondern dies auch mit der konkreten Maßnahme und Befugnis zu versehen, aus diesen 200 Teilprojekten eine Gemeinschaftsaufgabe zu machen.

Amt. Vors. **Josef Oster** (CDU/CSU): Herr Kob, die Zeit.

SV **Prof. Timo Kob** (HiSolutions): Gut, ich kann leider nicht so schnell lesen, wie Frau Griebsch, wir können hoffentlich nachtragen. Bundes-CISO – zweite wichtige Aufgabe.

Amt. Vors. **Josef Oster** (CDU/CSU): Vielen Dank, wir werden ja noch weiter Gelegenheit haben und Sie haben die Chance, auch Fragen zu bekommen, dann können Sie das weiter vertiefen. Wir machen weiter mit Herrn Kuhlenkamp, bitte.

SV **Felix Kuhlenkamp** (Bitkom): Sehr geehrter Herr Vorsitzender, sehr geehrte Abgeordnete, vielen Dank für die Gelegenheit, hier im Innenausschuss zur Umsetzung der NIS-2-Richtlinie Stellung zu nehmen. Der Bitkom und die Digitalwirtschaft unterstützen ausdrücklich die Ziele von NIS-2 für einheitliche europäische Sicherheitsstandards und eine gestärkte digitale Resilienz. Unsere aktuelle Wirtschaftsschutzstudie hat gezeigt, dass der Schaden durch Cyberangriffe in der deutschen Wirtschaft im vergangenen Jahr erstmals über 200 Milliarden Euro lag. Die Ziele der europäischen Richtlinie sind also nicht nur richtig, sie sind überfällig! Doch wir stehen unter erheblichem Zeitdruck. NIS-2 hätte bereits im Oktober 2024 in nationales Recht umgesetzt sein müssen. Jeder weitere Monat Verzögerung führt zu Strafzahlungen wegen Vertragsverletzungen und erhöht die Unsicherheit für Unternehmen. Andere Mitgliedstaaten sind bereits deutlich weiter. Dadurch entwickeln sich unterschiedliche Anforderungen, die grenzüberschreitende Tätigkeiten erschweren. Eine Eins-zu-eins-Umsetzung der europäischen Vorgaben ist also nicht nur eine Frage der Praktikabilität, sondern auch der Wettbewerbsfähigkeit. Zusätzliche nationale Regelungen oder Gold-Plating würden diesen Zielen zuwiderlaufen. Änderungen, die über NIS2-Vorgaben hinausgehen, sollten nur nach gründlicher Konsultation mit betroffenen Branchen oder in eigenständigen Gesetzgebungsverfahren erfolgen. Der verbleibende Gesetzgebungsprozess sollte stattdessen für eine rechtssichere Präzisierung des vorliegenden Entwurfs genutzt werden.

Dafür möchte ich drei konkrete Beispiele geben. Erstens besteht Unsicherheit, welche Unternehmen künftig konkret vom Gesetz erfasst sind. § 28 des Gesetzentwurfs möchte Unternehmen, die beispielsweise eine Ladesäule für Mitarbeitende betreiben oder intern Photovoltaik einsetzen, aus dem Anwendungsbereich herausnehmen – ein richtiger und wichtiger Ansatz. Es braucht jedoch fest definierte Schwellenwerte, um vernachlässigbare Geschäftstätigkeiten eindeutig zu definieren.

Zweitens sollten laufende Nachweisverfahren kritischer Infrastrukturen, die innerhalb von zwölf Monaten nach Inkrafttreten des neuen Gesetzes fällig sind, noch nach bisherigem Recht möglich sein.

Drittens ist eine enge Harmonisierung mit bestehenden Regelwerken unerlässlich, insbesondere mit dem KRITIS-Dachgesetz und der DSGVO. Die Bußgeldregelungen müssen klar definiert werden, um zu vermeiden, dass für denselben Verstoß mehrere Sanktionen verhängt werden können. Einheitliche Begriffsdefinitionen, abgestimmte Nachweiszyklen und gemeinsame Meldeverfahren sind notwendig, damit sich Unternehmen im Krisenfall auf Bewältigung statt auf Bürokratie konzentrieren können.

Zum Abschluss möchte ich einen Punkt betonen, der bereits von Timo Kob und auch anderen Sachverständigen adressiert wurde: Die nachgelagerten Bundesbehörden müssen in den Anwendungsbereich von NIS-2 fallen. Ansonsten entsteht nicht nur ein Glaubwürdigkeitsproblem gegenüber den regulierten Unternehmen, sondern, und das muss man leider so deutlich sagen, dann entsteht ein demokratiegefährdendes Sicherheitsrisiko. Mindeststandards reichen nicht aus, um uns vor den täglichen Angriffen auf die digitalen Infrastrukturen zu schützen. Der CISO Bund muss die Befugnisse erhalten, einheitliche Standards verbindlich zu überprüfen und durchzusetzen – auf allen Verwaltungsebenen! Vielen Dank für die Aufmerksamkeit. Weitere Details entnehmen Sie bitte der schriftlichen Stellungnahme des Bitkom.

Amt. Vors. **Josef Oster** (CDU/CSU): Vielen Dank, Herr Kuhlenkamp. Und als letzter in dieser Runde der Sachverständigen hat der Professor Dr. Schröder das Wort.

SV **Prof. Dr. Meinhard Schröder** (Universität Passau): Sehr geehrter Herr Vorsitzender, sehr geehrte Damen und Herren, vielen Dank für die Einladung. Ich freue mich sehr, hier Stellung nehmen zu können. Dass wir mehr für die IT-Sicherheit tun müssen, steht, glaube ich, außer Frage, das haben ja alle schon gesagt. Was zu tun ist, ist primär eine politische Frage. Aber es gibt dafür einen rechtlichen Rahmen, nämlich das Grundgesetz und das Europarecht. Und aus diesem Rahmen möchte ich in meinem Einführungsstatement auf drei Punkte kurz eingehen.

Zunächst die Umsetzung der Richtlinie im Bereich der Verwaltung: Mit der NIS-2-Richtlinie wollte

der europäische Gesetzgeber ja gerade den Kreis derjenigen, die besonders auf IT-Sicherheit achten müssen, erweitern, und er hat deswegen die Verwaltung mit einbezogen. Die korrekte Umsetzung der Richtlinie ist in diesem Bereich besonders wichtig, weil bereits ein Vertragsverletzungsverfahren gegen Deutschland eingeleitet ist und etwaige Fehler daher früher als sonst zu Strafzahlungen führen können. Aber lassen Sie sich nicht hetzen, auch hier geht Gründlichkeit vor Schnelligkeit, denn Strafzahlungen müssen erst einmal durch den EuGH verhängt werden. Wo liegen die konkreten Probleme? Der Entwurf erfasst entsprechend der grundgesetzlichen Kompetenzverteilung nur die Bundesverwaltung, das ist klar. Den Rest müssen Ihre Kollegen in den Ländern erledigen. Der Begriff der Bundesverwaltung wird im Entwurf im Ausgangspunkt richtlinienkonform definiert. Aber welche Vorschriften für die einzelnen Einrichtungen gelten, variiert dann doch erheblich. Und das führt meines Erachtens dazu, dass einzelne Vorgaben der Richtlinie nicht korrekt umgesetzt werden. Das gilt vor allem für die Pflicht zum Risikomanagement, das für die Verwaltung durch die Befolgung von BSI-Standards nach § 44 des Entwurfs ersetzt wird. Erstens ist fraglich, ob man die Richtlinie überhaupt so umsetzen kann. Zweitens ist der Standard, den die Bundesverwaltung abseits der Ministerien und des Kanzleramts einhalten muss, ziemlich sicher zu niedrig. Das haben wir schon mehrfach gehört. Drittens stellt sich die Frage, warum für den öffentlichen Sektor überhaupt andere Standards gelten sollen als für sehr wichtige private Einrichtungen. Außerdem gehen wohl auch die Ausnahmen für das Auswärtige Amt zu weit.

Ein zweiter Punkt, auf den ich eingehen möchte, jenseits der Richtlinienumsetzung, ist die Untersagung des Einsatzes kritischer Komponenten: Eine solche Kompetenz zu haben, kann durchaus sinnvoll und auch unter Umständen verfassungsrechtlich geboten sein. Die konkrete Regelung weist aber verschiedene problematische Elemente auf. Einerseits sind die Voraussetzungen so vage, dass eine Untersagung wohl mehr durch politische Erwägung als durch solche der IT-Sicherheit geprägt wäre. Andererseits scheint bei Ausbauanordnungen die Vollzugstauglichkeit zweifelhaft – ich stelle es mir nicht leicht vor, das Einvernehmen mit elf Ressorts herzustellen.

Dritter und letzter Punkt, das Schwachstellenmanagement, auch das wurde schon angesprochen: Das BSI darf nach dem Entwurf scannen, ob bei Einrichtungen bekannte Schwachstellen vorliegen – das ist sicher gut. Nicht geregelt ist aber, wie mit Sicherheitslücken umzugehen ist, von denen das BSI oder eine andere Stelle der Bundesverwaltung zufällig erfährt. Hier sollte man einerseits dafür sorgen, dass solche Meldungen nicht aus Angst vor Strafe unterbleiben und andererseits im Einklang mit den Vorgaben des Bundesverfassungsgerichts von 2021 regeln, wann die Hersteller über Schwachstellen informiert werden müssen und wann der Staat das Wissen für eigene legitime Zwecke nutzen darf. Für weitere Punkte darf ich auf meine Stellungnahme verweisen und auf eventuelle weitere Fragen. Vielen Dank.

Amt. Vors. **Josef Oster** (CDU/CSU): Vielen Dank auch Ihnen, Herr Professor Dr. Schröder. Wir sind damit mit den Eingangsstatements zum Abschluss gekommen. Ich bitte um Nachsicht oder Verständnis, dass ich da ein bisschen streng bin, was die Zeitlimits betrifft. Aber ich glaube, Ihre Stellungnahmen haben gezeigt, wie viel es hier zu besprechen gibt, wie vielfältig die Facetten sind, die hier zu erörtern sind. Deswegen wollen wir jetzt auch in die Fragerunde der Fraktionen einsteigen. Wir haben nicht nur Innenausschuss-Kolleginnen und -kollegen hier, deswegen noch einmal ganz kurz zum Verfahren: Wir haben im Innenausschuss das System, dass jede Fraktion in jeder Runde zwei Minuten bekommt und in diesen zwei Minuten jeweils eine Frage an zwei Sachverständige richten kann oder zwei Fragen an einen Sachverständigen und dafür haben Sie zwei Minuten Zeit und darauf wird dann auch von dem Sachverständigen oder der Sachverständigen unmittelbar geantwortet. So, das zum Verfahren und wir beginnen mit der Unionsfraktion und der Kollege Schmidt hat das Wort.

Abg. **Henri Schmidt** (CDU/CSU): Sehr geehrter Herr Vorsitzender, vielen Dank für die Möglichkeit, eine Frage zu stellen. Erst einmal freue ich mich, dass wir alle in die gleiche Richtung denken. Allen ist das Thema Cybersicherheit extrem wichtig, auch wenn wir vielleicht im Detail noch den einen oder anderen Punkt zu klären haben. Viele der Punkte, die wir heute gehört haben, sind Gott sei Dank auch in unseren Vorgesprächen abgeordnetenseitig schon einmal Thema gewesen, sodass wir also glauben, dass wir in vielen Bereichen auch

sehr gut zusammenkommen. Ich selbst bin heute hier nicht als Mitglied des Innenausschusses, sondern als Berichterstatter für die Cybersicherheit des Bundes und vor diesem Hintergrund möchte ich mich insbesondere noch einmal über die Rolle des CISOs unterhalten. Hintergrund ist, dass ich diverse Erfahrungen aus Unternehmen mitbringe und die Rolle des CISOs in den letzten Jahren habe wachsen sehen von einer, ich sage einmal Rolle, die geschaffen wurde, hin zu einer immer strategischeren Rolle, weil einfach das Thema Cybersicherheit an Bedeutung gewonnen hat. Und genau vor diesem Hintergrund würde ich gern das Thema CISO des Bundes thematisieren und richte meine Frage gern an Professor Kob und Herrn Gehringer. Es geht mir um Ihre Einschätzung und Ihr Wissen aus der Wirtschaft oder aus vergleichbaren Komplexen, wie ein CISO denn eingesetzt wird. Welche Rolle sollte er aus Ihrer Sicht haben, welche Rechte und Möglichkeiten, vielleicht auch Berichtspflichten und vor allen Dingen auch, welche Dinge sollten wir dringend vermeiden?

Amt. Vors. **Josef Oster** (CDU/CSU): Vielen Dank, Herr Schmidt. Das ist eine Frage an zwei Sachverständige. Beide haben jeweils zwei Minuten Zeit, das zu beantworten und wir machen das in alphabetischer Reihenfolge und beginnen mit Herrn Gehringer.

SV **Ferdinand Gehringer** (Konrad-Adenauer-Stiftung): Wunderbar, vielen Dank für die Frage. Der CISO hat in der Regel ein klares Mandat. Ich würde es zunächst auf vier Punkte reduzieren: Klare Mandate und Verantwortlichkeiten sowie die Abgrenzung zu anderen Tätigkeiten. Er ist entweder von der Geschäftsführung oder vom Vorstand damit beauftragt, die IT-Sicherheitsstrategie voranzutreiben und hat Vetorechte bei sicherheitskritischen Prozessen. Das heißt der CISO Bund braucht ein gesetzlich verankertes Mandat, das seine Rolle und Verantwortlichkeiten und seine Befugnisse klar definiert. Er sollte die Federführung bei nationalen Cyberkrisen haben. Und er ist Manager und Sicherheitsbeauftragter zugleich.

Zweitens: Unabhängigkeit und direkte Berichtslinie. Effektive CISOs berichten direkt an die Geschäftsführung oder an den Vorstand, um Interessenkonflikte zu vermeiden. Der oder die CISO Bund sollte einen direkten Zugang zur Bundesregierung oder einem Minister haben. Fachkundigkeit und Praxisnähe sind dabei entscheidend. Diese beiden Komponenten in Einklang zu bekommen und zusätzlich den Zugang zum entsprechenden Ministerium zu bekommen, ist das entscheidende Maß bei der Positionierung des CISO Bund. Fachliche und sachliche Qualifikationen sowie die Erfahrung mit der Informationssicherheit sind hierbei entscheidend. Demnach wären Berichtspflichten gegenüber dem Bundesrechnungshof und dem Deutschen Bundestag und den dort zuständigen Ausschüssen ratsam.

Drittens: Ressourcen und Durchsetzungsmacht. CISOs in der Wirtschaft haben eigene Budgets und können Sicherheitsstandards verbindlich durchsetzen. Der CISO Bund braucht eigene Haushaltsmittel und die Befugnis verbindliche Sicherheitsstandards in allen Bundesbehörden vorzugeben, inklusive Sanktionierungsmöglichkeiten bei Nicht-Einhaltung.

Viertens: Die Zusammenarbeit mit anderen Akteuren. Erfolgreiche CISOs arbeiten eng mit IT-Abteilungen, Risikomanagement, Compliance-Abteilungen und externen Beratern zusammen. Demnach sollte der CISO Bund eine Schnittstelle zwischen anderen Akteuren im Rahmen der deutschen gesamtheitlichen Cybersicherheitsarchitektur sein – das bedeutet Bundesbehörden, Länder, kritische Infrastrukturen, die Privatwirtschaft, aber auch internationale Partner.

Amt. Vors. **Josef Oster** (CDU/CSU): Vielen Dank, Herr Professor Kob.

SV **Timo Kob** (HiSolutions): Ich bilde das Ganze einmal ab, wie man es im Unternehmen etablieren würde, was da die Fragestellungen sind. Und dann sind es eigentlich zwei Knackpunkte: die Durchsetzungskraft und die Zielkonflikte. Ich würde jetzt einmal die Szenarien abbilden, die hier im Raum herumgeistern: Das Hauptproblem, mangelnde Durchsetzungskraft, greift immer dann, wenn ich zu weit von den Entscheidungsträgern entfernt bin. Wenn ich also an das BSI denke, wäre es das größte Problem, dass es nachgeordnete Behörde ist. Da hat die AG KRITIS unter anderem gefordert, aber es war auch im politischen Raum, dass sogar das Bundeskanzleramt das machen soll. Das wäre natürlich nächstmöglich an den Entscheidungen, aber führt auch zu einer gewissen Elfenbeinturm-Problematik. Dazwischen stehen die beiden Ministerien. Da ist aber ebenfalls auch das, was Ferdinand Gehring gesagt hat, ob ein Staatssekretär

überhaupt die entscheidende Ebene ist. Es muss in irgendeiner Weise einen Weg an den Kabinettstisch durch über Berichtspflichten, Eskalationswege etc. gehen.

Das zweite Thema ist das Thema Zielkonflikte. Das BSI hat natürlich die geringsten Zielkonflikte, das steckt im Namen, da geht es um Sicherheit. Der größte Zielkonflikt wäre dann beim BMDS, weil Digitalisierung und Sicherheit eben oft genug im Widerspruch zueinanderstehen. Da hätten wir natürlich umgekehrt beim Bundeskanzleramt auch keine größeren Zielkonflikte. Aber alle Varianten haben einen Pferdefuß. Alle sind machbar. Alle Probleme sind auch heilbar.

Also in der Wirtschaft würde man gucken, was jetzt der passende Vorstand wäre. Dann würde man sagen nach Wirkmacht vielleicht eher wie ein Finanzvorstand statt Personalvorstand. Da könnte man jetzt auch die Politik ableiten, eher ein A-Ministerium als ein B-Ministerium. Umgekehrt muss man auch gucken, was potentiell die Wirkhebel sind, da könnte das BMDS mit dem Thema Budgetvorbehalt punkten, wichtig ist aber: Das moderne Bild heißt *weniger* Revisor, *mehr* Berater – deswegen mehr operative Kenntnisse. Deswegen würde ich bei all den Bauchschmerzen, die ich trotzdem habe, dann aus der Erfahrung am ehesten in Richtung BSI gehen, um es eben nicht nur, wie im Eingangsstatement erwähnt überhaupt sondern auch effizient sicher zu machen. Berater für diese 200 Teilprojekte zu sein, wäre dann für mich sozusagen der ausschlaggebende Hebel, wobei alle Varianten denkbar sind. Wichtig ist: Irgendwo muss es an den Kabinetttisch, sprich, wenn der CISO beim BSI wäre, dann brauche ich auf jeden Fall einen direkten Weg Deeskalationsweg zu einem Minister, welcher auch immer das ist.

Amt. Vors. **Josef Oster** (CDU/CSU): Vielen Dank. Wir fahren fort mit der AfD-Fraktion. Und das macht Herr Janich, bitte.

Abg. **Steffen Janich** (AfD): Ja, vielen Dank, Herr Vorsitzender. Meine erste Frage geht an Herrn Gehringer und die zweite an Frau Griebsch. Herr Gehringer, Sie haben in Ihrem Eingangsstatement betont, dass man Chancen nutzen soll, Anreize für kleine und mittlere Unternehmen setzen, um hier mit einer gewissen Freiwilligkeit vermutlich dann in die Sache einzudringen. Wie stellen Sie sich die Anreize, die seitens NIS-2 gesetzt werden sollen, vor? Könnte man da sagen, dass die Umsetzung der NIS-2-Richtlinie aus Ihrer Sicht gerade bei solchen Bevorteilungen vielleicht dann Unternehmensinsolvenzen reduzieren könnte? Wo sehen Sie da Ansätze, dass wir unsere kleinen und mittleren Unternehmen hier in dieses Projekt mit einbeziehen können?

Und meine zweite Frage geht an Frau Griebsch: Sie haben davon gesprochen, dass Sie über die kommunale Ebene Ihre ganze Sachkompetenz hier mit einbringen und sprachen von der Einbeziehung der Kommunen und sehen dort auch kritische Lücken. Mich würden schon interessieren, wo die kritischen Lücken sind. Wir wissen ja, unsere Kommunen sind in ihren Haushalten trocken wie ein Tequila, das ist halt so. Wie sehen Sie die Möglichkeit, in den Kommunen dann die NIS-2-Umsetzung voranzubringen, um dort auch wirklich realistische Konzepte zu erzielen? Vielen Dank.

Amt. Vors. **Josef Oster** (CDU/CSU): Danke. Zwei angesprochene Sachverständige. Zuerst Herr Gehringer und dann Frau Griebsch.

SV **Ferdinand Gehringer** (Konrad-Adenauer-Stiftung): Zum Thema Chancen nutzen ist es so, dass die NIS-2- Richtlinie den Aufbau einer umfassenden Plattform anregt und dementsprechend dem BSI auferlegt, wo die Informationen, die man über die Cyber-Sicherheitslage entwickelt, die man aus den Meldungen heraus entwickelt, erfasst werden. Diese Plattform bietet die einmalige Chance, sich so von Grund auf so aufwerten zu lassen, dass man sie eben auch nicht meldepflichtigen Unternehmen, die dementsprechend erst einmal keinen Meldedrang aufgrund der gesetzlichen Grundlage verspüren, trotzdem anbieten kann, indem man auf dieser Plattform beispielsweise, sobald man eine Meldung vornimmt, sofort im Gegenzug Informationen gibt – also Erstkontakte, Erste-Hilfe-Maßnahmen, irgendwelche IT-Dienstleister-Kontakte, sofortige Notfallmaßnahmen, die dann für kleinere Unternehmen, besonders in den ersten paar Minuten, in den ersten Stunden besonders hilfreich sein können, damit sie sich sofort mit diesen Vorgängen beschäftigen können. Das könnte eine Anreizfunktion haben, um an dieser Plattform zu partizipieren, um dadurch auch automatisch besser an Informationen zu kommen, ohne dass eine gesetzliche Verpflichtung kommt, ohne dass sie einer gesetzlichen Verpflichtung unterliegen. Das hätte, angesichts der Tatsache, dass wir derzeit sehr viele

Lieferkettenangriffe sehen, und auch kleinere Unternehmen entlang der Lieferkette betroffen sind, den Charme, dass man diese relativ niedrigschwellig durch ein Angebot integrieren könnte, was sowieso geschaffen werden muss.

SVe **Sabine Griebsch** (GovThings): Vielleicht von mir die kurze Antwort: Also aus der Erfahrung ist es tatsächlich der Fall, dass wir in mehreren Kommunen tatsächlich auf der einen Seite die Meldepflichten haben, also aktuell senden Kommunen in das Lagebild, wenn, also aktuell eher freiwillig und das bedeutet, dass wir gerade eine Einbahnstraße und keine Rückmeldung haben. Also Kommunen haben keinen Zugriff aufs Lagebild, das heißt also in der Verantwortung – die Kommunen haben die Cyberabwehr eben auch in den Kommunen vorzunehmen – sind wir aktuell blind. So, das ist das eine.

Auf der anderen Seite haben wir die Problematik, dass durch diese Zerstückelung durch den Föderalismus in den Bundesländern andere Vorgaben herrschen, wir uns auf der einen Seite an die Polizei wenden und auf der anderen Seite auch immer noch an das BSI, natürlich auch an die Länder, also die Kommunen hängen an den Netzen der Länder. Das heißt also die Landes-CERTs (Computer Emergency Response Team) sind immer erster Ansprechpartner, auch für die Kommunen und die Polizei. Die Problematik ist dabei aber, dass diese Meldepflichten immer wieder an allen möglichen Orten entstehen und der Aufwand in der ersten Phase des Vorfalls, wenn ich ihn bemerkt habe, immens hoch ist und im Anbetracht der wenigen Personen, die ich dann vor Ort habe, das natürlich in der Bearbeitung wahnsinnig auffällt.

Und dann pflegen wir andererseits unseren Flickenteppich. Also wenn ich die Kommunen nicht mit einbeziehe, dann führt das natürlich dazu, dass die Kommunen als schwächstes Glied immer angreifbar bleiben und zwar an der Schnittstelle hin zum Bürger. Ich hatte in der Stellungnahme einen Sachstandsbericht des wissenschaftlichen Dienstes des Bundestages herangezogen. Der hat klargestellt, dass die Aufnahme von Kommunen gemäß Artikel 2, Absatz 5, Ziffer 5 a) NIS-2-Richtlinie rechtlich zulässig ist. Und das bedeutet, der Gesetzgeber hat aktuell von dieser Option noch keinen Gebrauch gemacht. Ich plädiere aber absolut dafür, dies zu tun, damit Kommunen eben unter dieses Schutzschild geraten!

Amt. Vors. **Josef Oster** (CDU/CSU): Vielen Dank für die Beantwortung dieser beiden Fragen. Ich darf die parlamentarische Staatssekretärin Daniela Ludwig begrüßen. Sie waren etwas verspätet angekündigt, deswegen freuen wir uns, dass Sie jetzt da sind und wir können in der Fraktionsrunde fortfahren. Für die SPD-Fraktion hat Herr Schätzl das Wort.

Abg. **Johannes Schätzl** (SPD): Sehr geehrter Herr Vorsitzender, sehr geehrte Frau Staatssekretärin, im Sinne des Verfahrensvorschlags würden wir zwei Fragen an jeweils einen Sachverständigen stellen, und, insofern Sie es erlauben, uns die Fragen in der Fraktion teilen. Die erste Frage geht an Herrn Dr. Herpig mit Blick auf die angespannte auch geopolitische Sicherheitslage, mit Blick auf § 9 bzw. den neuen § 41 BSIG. Ich stelle für mich fest, dass das ja doch aktuell eher ein stumpfes Schwert ist. Die Frage, die ich gern an Sie richten würde, ist, welche Änderungen würden Sie denn vorschlagen im Bereich § 41 BSIG, um einen rechtssicheren Ausschluss kritischer Komponenten von nicht vertrauenswürdigen Anbietern vornehmen zu können?

Abg. **Daniel Baldy** (SPD): Die zweite Frage meiner Fraktion würde sich, Herr Professor Dr. Schröder, an Sie richten. Bei den vorab eingegangenen Stellungnahmen ging es auch häufiger um den § 28 BSIG und das Thema des vernachlässigbaren Geschäftsbereichs. Wie würden Sie das denn aus der Sicht der Forschung sehen? Da gibt es die unterschiedlichsten Vorschläge – von konkretisieren bis ganz weglassen. Da würde mich interessieren, wie das denn aus Sicht der Forschung aussieht? Wie sollen wir es machen?

Amt. Vors. **Josef Oster** (CDU/CSU): Vielen Dank für die Fragen. Zunächst hat Herr Dr. Herpig das Wort, digital zugeschaltet, und dann Herr Professor Dr. Schröder. Herr Dr. Herpig.

SV **Dr. Sven Herpig** (interface): Wunderbar, vielen Dank. Ich glaube, es gibt eine ganze Reihe an Sachen, die man noch einmal angucken müsste, zum einen, § 2 Ziffer 23 BSIG, das ist eine sehr starre Begriffsdefinition von kritischen Komponenten, die sich sehr schwer anpassen lässt, nicht so flexibel ist, wie wir es in der geopolitisch dynamischen Lage eigentlich bräuchten. Wenn wir dann in § 41 BSIG hineingucken, sehen wir eigentlich eine Bürokratiemonster: Es muss eine Garantieerklärung

abgegeben werden, das wird Papierhaufen ergeben, die irgendwo gestapelt werden müssen. Keines der Unternehmen oder kaum eines der Unternehmen kann nachhalten, über welche Infrastrukturen und welche Firmengebilde sich irgendwelche Komponenten zusammensetzen. Allein schon mit Blick auf den wachsenden chinesischen Markt von Softwarekomponenten, von KI-Unternehmen und so weiter – Sie kennen es ja alles – ist es schwer nachvollziehbar, wo welche Komponenten herkommen und wie die denn abgesichert sind. Es gibt Länder, ohne sie dezidiert zu nennen, wo Huawei-Produkte ausgeschlossen sind, die aber unwissentlich über eine Dritttochterfirma dann doch Produkte von Huawei einkaufen, weil sie nicht nachverfolgen konnten, dass Huawei da irgendwie noch mit hineinspielt. Von daher ist diese Garantieerklärung nicht viel mehr als ein großer Papierhaufen.

Das Gleiche gilt für die Anzeigepflicht: Man hat zwei Monate, um zu antworten. Kein Angriff gegen die Kolleginnen und Kollegen aus dem BMI, aber das wird kaum leistbar sein, das vernünftig abzuarbeiten. Wenn man dann noch ins Einvernehmen gehen muss, und Professor Dr. Schröder hat es schon angesprochen, mit bis zu elf Bundesministerien, da werden Sie überhaupt nichts hinbekommen, außer dass es Abstimmungsrunden über Abstimmungsrunden gibt mit hunderten seitenlangen „Ergebnis-PDFs“, die auch nicht vollständig sein können und nicht sind, nur damit man sagt, man hat etwas getan, um sich abzusichern. Alle diese Punkte müsste man angehen, teilweise werden aber auch Punkte wie in § 41 Absatz 5 Satz 4 BSIG, was die Schwachstellen angeht, bereits auch parallel über den Cyber Resilience Act abgebildet werden. Das heißt, ich bin der Meinung, man muss an den kompletten § 41 BSIG und teilweise vielleicht auch noch einmal an § 2 Ziffer 23 heran und diese entsprechenden Punkte überarbeiten. Vielen Dank.

Amt. Vors. **Josef Oster** (CDU/CSU): Danke. Herr Professor Schröder.

SV **Prof. Dr. Meinhard Schröder** (Universität Passau): Vielen Dank für die Frage. Ich würde meine Antwort zweiteilen wollen, einmal auf die juristische Perspektive eingehend, was meine primäre Expertise ist. Da sehe ich ehrlich gesagt nicht, dass die NIS-2-Richtlinie eine Öffnungsklausel enthält, nach der man diese Ausnahme so, wie sie hier drinsteht, vornehmen kann. Und damit bin ich schon ein bisschen bei der zweiten Perspektive. Ich habe mich in Vorbereitung dieser Stellungnahme mit einem Kollegen von unserem Passau Institute of Digital Security, einem Informatiker aus dem Sicherheitsbereich, ausgetauscht. Der hat mich darin bestärkt, dass es eigentlich nur um die Kritikalität gehen darf. Wenn ein Unternehmen auch nur als unwesentlichen Bestandteil seiner Geschäftstätigkeit einen solchen kritischen Dienst anbietet, dann muss es diesen Vorgaben unterworfen sein. Und aus juristischer Sicht sehe ich auch nicht, dass die NIS-2-Richtlinie das so vorsieht, daher würde ich tatsächlich dafür plädieren, diese Ausnahme einfach zu streichen.

Amt. Vors. **Josef Oster** (CDU/CSU): Danke schön. Es geht weiter mit der Fraktion BÜNDNIS 90/DIE GRÜNEN, Herr Dr. von Notz.

Abg. **Dr. Konstantin von Notz** (BÜNDNIS 90/DIE GRÜNEN): Herr Vorsitzender, vielen Dank. Vielen Dank an die Expertinnen und Experten für die Expertise und die Zeit und die Eindeutigkeit Ihrer Stellungnahmen. Die Staatssekretärin ist einen Moment zu spät gekommen, aber ich kann sehr anraten, die Stellungnahmen alle zu lesen. Denn das ist schon frappierend, sage ich einmal, dass wir hier jetzt in genau der gleichen Ausgangslage stehen wie vor einem Jahr! Wenn Sie sich das angucken, die Punkte Schwachstellenmanagement, CISO Bund, das sind alles Dinge, die wir vor einem Jahr diskutiert haben, und ich finde es einfach krass, dass das BMI so einen Entwurf vorlegt – ich muss das jetzt einmal loswerden. Und wie das zusammenkommen soll, da bin ich sehr gespannt. Ich habe die steilen Reden auch aus der Koalition im Plenum gehört – wir werden sehen!

So, ich habe aber auch eine Frage, und zwar bezieht sie sich auf das Schwachstellenmanagement, das man vielleicht einmal den Menschen „außen“ auch erklären muss. Die Diskrepanz zwischen der Notwendigkeit, wo, glaube ich, hier viele sehen, dass man in manchen Situationen eventuell auch Schwachstellen nutzen möchte und gleichzeitig der unter Cyber-Sicherheitsgesichtspunkten absoluten Notwendigkeit, relevante Schwachstellen zu schließen. Deswegen würde ich gern Herrn Professor Kipker und Herrn Gehringer fragen, wie Sie auf diese Herausforderungen gucken und wie man das am besten aufgelöst bekommt. Denn im augenblicklichen Gesetzentwurf wird dieses Problem nicht aufgelöst. Und ich glaube, wir können uns

angesichts der Cyberangriffe, denen Deutschland jeden Tag ausgesetzt ist und die einen Schaden von mindestens 250 Milliarden Euro im Jahr verursachen, nicht leisten, einfach random Sicherheitslücken offen zu halten, ohne zu prüfen, wie gravierend die Flanke ist, die wir damit aufmachen.

Amt. Vors. **Josef Oster** (CDU/CSU): Danke, dann mache ich das in der Reihenfolge, wie Sie sie genannt haben und ich erteile zunächst Professor Dr. Kipker das Wort und dann Herrn Gehringer.

Prof. Dr. Dennis-Kenji Kipker (Universität Bremen): Vielen Dank. Das ist in der Tat ein sehr wichtiger Punkt. Und das staatliche Schwachstellenmanagement ist nicht nur etwas, was irgendwie allgemein über uns schwebt, sondern das ist eine verfassungsrechtliche Vorgabe. Denn der Staat hat natürlich auch eine Schutzpflicht, Cybersicherheit zu schaffen und diese Schutzpflicht ist grundrechtlich verankert! Es gibt bereits seit mehreren Jahren ein sogenanntes Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme. Das Bundesverfassungsgericht hat schon im Jahr 2008 argumentiert, und das war im Jahre 2008, als wir noch nicht groß über Cloud-Computing und Smartphones gesprochen haben, dass quasi die Computer und eben auch die vernetzte IT, das digitale Gedächtnis nicht nur von natürlichen Personen, sondern auch von Unternehmen abbilden. Und gleichzeitig ist es auch so, das ist auch eine Debatte, die wir mehr und mehr im digitalen Raum sehen, und die hat nicht unbedingt mit NIS-2 zu tun, sondern generell mit der Sicherheit des digitalen Raums, dass natürlich auch klassisch Freiheitsrechte ohne digitale Sicherheit nicht vernünftig ausgeübt werden können – das meint vor allem natürlich auch die Meinungsfreiheit. Und diese Schutzpflicht, die man eben aus verschiedenen verfassungsrechtlichen Gewährleistungen ableiten kann, die verlangt letzten Endes vom Staat nichts anderes, als die IT-Systeme von Bürgerinnen und Bürgern vor Cyberbedrohungen zu schützen! Und dazu gehört eine proaktive Identifizierung, Meldung und Beseitigung von Schwachstellen. Und das Offenhalten von Schwachstellen, gerade das bewusste Nichtschließen für geheimdienstliche, sicherheitsbehördliche, polizeiliche Zwecke, birgt gemessen an diesen verfassungsrechtlichen Gewährleistungen, natürlich erhebliche Risiken, weil es die Schutzpflicht des Staates irgendwo auch konterkariert. Und deswegen ist es dringend erforderlich, eben auch eine transparente Handhabung von Schwachstellen zu schaffen, das im Gesetz zu verankern, deren schnellstmögliche Beseitigung anzuordnen, gesetzlich im BSI-Gesetz insbesondere, und damit eben auch für die Hersteller eine Möglichkeit zu schaffen, Schwachstellen möglichst schnell zu beseitigen. Danke schön.

Amt. Vors. **Josef Oster** (CDU/CSU): Danke. Herr Gehringer.

SV **Ferdinand Gehringer** (Konrad-Adenauer-Stiftung): Vielen Dank für die Frage. Daran anknüpfend ist es immer eine Abwägung zwischen der Schutzpflicht des Staates und den Sicherheitsinteressen sowie den Interessen der Strafverfolgung und auch der Aufklärung. Ich plädiere aber anschließend an meinen Vorredner ganz klar auch dafür, dass man im Sinne des Schwachstellenmanagements klare, transparente Verfahren an den Tag legen muss, die es nicht ermöglichen, dass Schwachstellen über viele, viele Jahre hinweg offengehalten werden können. Gleichzeitig ist es so, dass die Meldungen von Schwachstellen ebenfalls einem gesicherten Verfahren unterstellt werden müssen, sodass sich Meldende nicht zurückhalten, Schwachstellen zu melden, dass wir klare Transparenz auch hinsichtlich der Schwachstellen bekommen können. Ob das Ganze jetzt so sinnvoll in der NIS-2 verortet werden kann: In Anbetracht der Dringlichkeit der Situation, die NIS-2 schnell umzusetzen und der Komplexität rund um die Verfahren und die Abwägungsprozesse im Sinne der Schwachstellen und des Schwachstellenmanagements, würde ich mich jetzt schwertun, das noch in die NIS-2 hineinzupacken und das nicht gesondert anzugehen, weil diese Interessenabwägung auch mit anderen Behörden gemeinschaftlich getroffen werden muss und vor allen Dingen sichere Meldevorgänge geschaffen werden müssen, die in diesem Zusammenhang wahrscheinlich nicht über die NIS-2 geschaffen werden können. Danke.

Amt. Vors. **Josef Oster** (CDU/CSU): Vielen Dank. Wir fahren fort mit der Fraktion Die Linke. Frau Vogtschmidt.

Abg. **Donata Vogtschmidt** (Die Linke): Vielen Dank. Meine zwei Fragen richten sich an Frau Griebsch. Vielen Dank für Ihre ausführliche Stellungnahme. Es hat uns sehr gefreut, die dann auch zu lesen und dort Inhalte zu entnehmen. Der IT-Planungsrat

hat ja argumentiert, dass die IT-Sicherheit der Kommunen vom Bund besser nicht geregelt werden solle, unter anderem, um Kommunen nicht zu stark unter Druck zu setzen und auch die Zuständigkeit nicht infrage zu stellen. Überzeugt Sie das auch aus Ihrem Werdegang und auch mit Blick auf das Thema Staatsmodernisierung und Etablierung von Standards oder auch dem Abbau von Regelungswildwuchs?

Und meine zweite Frage wäre: Wenn Sie jetzt auch auf die Gesamtsituation blicken – gerade in Abwägung mit der Tatsache, dass hier jeder Tag ohne die NIS-2-Umsetzung ein Tag erhöhter IT-Unsicherheit ist – halten Sie das Verbesserungspotenzial im aktuellen NIS-2-Entwurf so groß, dass es im Zweifel dann doch besser wäre, die Verabschiedung des Gesetzesentwurfs noch etwas abzuwarten und Zeit für substanzielle Verbesserungen zu schaffen oder nicht? Danke.

Amt. Vors. **Josef Oster** (CDU/CSU): Vielen Dank. Das sind zwei Fragen an eine Sachverständige, Sie haben somit vier Minuten Zeit, darauf zu antworten. Frau Griebsch, bitte.

SVe **Sabine Griebsch** (GovThings): Also erstens ist es so, dass wir in den Kommunen verschiedene Situationen sehen. Das heißt, wir haben Kommunen, die mit Mitteln gesegnet sind, und wir haben Kommunen, die weitaus größere Probleme haben, ihre Digitalisierungsprojekte anzugehen oder mit Digitalisierungsprojekten, wenn ich jetzt gerade an meine Vergangenheit als CIO denke, wenn es dann mit einem Mal dazu kommt, das OZG umzusetzen, den „Digitalpakt Schule“ umzusetzen, öffentliches Gesundheitswesen umzusetzen und dann entsprechend die IT-Abteilung mit dem entsprechenden Personal zu überfordern. Und das bezieht sich natürlich auch auf das ganze Thema IT-Sicherheit, das natürlich in den letzten Jahren immens zugenommen hat. Wir haben auf der einen Seite den Hackerangriff auf Anhalt-Bitterfeld gesehen. Wir haben den Cyberangriff auf die Südwestfalen-IT (SIT) gesehen. Wir haben wahnsinnig viele andere Kommunen gesehen, die von absolut professionellen Gruppierungen angegriffen werden. Hier ist sozusagen die Grenze zwischen kommerziellen und politischen Angreifern fließend. Das heißt, Kommunen stehen dem gegenüber und können es tatsächlich nicht abwehren. Entsprechend in der aktuellen Situation – auf der einen Seite Länder, die IT-Sicherheitsgesetze bereits verabschiedet haben, andererseits Länder, die da tatsächlich noch in Planung sind – ist es so, dass bei Kommunen aktuell permanent diese Überforderung und diese Abwägung in der Frage, in der Überlegung, ist die Straße wichtiger, ist der Spielplatz wichtiger, natürlich immer wieder da ist. Das heißt natürlich, dass wir in der Versorgungssicherheit, in der kommunalen Daseinsvorsorge, die sich natürlich auch auf Themen wie Abfallentsorgung, Krankenhaus, Wasser und so weiter erstreckt, hier tatsächlich eine Situation haben, wo wir sagen müssen, dass das Gefälle zwischen den Regionen immens hoch ist. Und wenn ich daran denke, welche Daten von Bürgerinnen und Bürgern dort gefährdet sind, ob das höchstpersönliche Daten sind aus dem Bereich Gesundheit oder existenzielle Daten oder Leistungen, die aus dem Sozialbereich sind, dann führt das dazu, dass wir hier ein Gefälle haben und dass man hier natürlich tätig werden muss.

Die Länder haben aktuell teilweise freiwillige Angebote. Die Zuständigkeiten, die föderalen Zuständigkeiten, das ist problematisch. Das heißt, auch die Unterstützungsmöglichkeiten, die das Land den Kommunen bieten kann, sind immens verschie-den – und das darf nicht sein. Ich hatte es vorhin auch schon mit der Fragmentierung gesagt, die Kommunen sind aktuell auf sich allein gestellt, auch wenn ein IT-Grundschutz da ist. Und immer wieder die Abwägung, dass man sagt: Dann machen wir die Wege in die Basisabsicherung. Wir werden immer weiter zurückgestuft. Das führt dazu, dass Kommunen dort nicht vorankommen.

Ich muss noch einmal kurz nach der zweiten Frage fragen. Ach so, genau, diese Verwässerung, dieses Verwässerungspotenzial. Wir gucken nicht nur auf die Kommunen. Wir gucken auch auf den Bundesbereich. Das heißt natürlich, dass, wenn ich das richtig verstanden habe, dass diese Abstufung hin zu nachgeordneten Bereichen dazu führt, dass auch hier immer wieder Angriffsmöglichkeiten geschaffen werden. Und ich kann nicht in Worte fassen, wie schwierig das ist, hier einfach keine Handhabe zu haben, diese Bereiche dorthin zu führen, wenigstens das Mindestmaß an Schutzmaßnahmen umzusetzen. Das war es schon von mir.

Amt. Vors. **Josef Oster** (CDU/CSU): Vielen Dank, Frau Griebsch. Damit sind wir mit der ersten Fragerunde durch und ich würde in die zweite einsteigen in der gewohnten Fraktionsreihenfolge.

Und für die CDU/CSU gebe ich das Wort Herrn Henrichmann. Bitte.

Abg. **Marc Henrichmann** (CDU/CSU): Vielen Dank, Herr Vorsitzender. Ich würde gern Herrn Kob und Herrn Kuhlenkamp eine Frage stellen. Sie haben sehr deutlich die nachgelagerte Bundesverwaltung, die Bundesbehörden adressiert. Darauf möchte ich noch einmal eingehen. Und zwar: Wir rennen damit ganz offene Türen ein, weil wir auch über so was reden wie die Netze des Bundes, über die dann im Idealfall alle gemeinsam kommunizieren, was denknotwendig nur funktionieren kann, wenn man auch irgendwie ein gemeinsames Schutzniveau hat. Und ganz aberwitzig wird es dann, wenn man sich vorstellt, dass BKA oder BSI selbst sozusagen schludern könnten bei den Sicherheitsanforderungen. Aber deswegen, Herr Kuhlenkamp, mit Blick auf die Wirtschaft, die Sie als Bitkom vertreten: Wie ist denn da die Wahrnehmung? Man fordert jetzt der Wirtschaft in diesem Bereich etwas ab, sagt aber dann als Gesetzgeber im Zweifel, bei der Bundesverwaltung ist es aufwendig oder teuer oder beides. Und Professor Kob, Sie haben ja auch die Kostensituation ein bisschen beleuchtet aus Ihrer beruflichen Erfahrung. Und was wir so wissen, wenn das UP-Bund-Niveau umgesetzt wäre, möchte ich in Vergleich setzen zu NIS-2. Und wie groß wäre denn der Sprung, wenn UP Bund, der eigentlich als Level erreicht sein müsste, erreicht wäre, zu dem, was NIS-2 jetzt obendrauf abverlangt – wie weit, wie groß wäre der Schritt?

Amt. Vors. **Josef Oster** (CDU/CSU): Vielen Dank. Herr Kob und dann Herr Kuhlenkamp.

SV **Prof. Timo Kob** (HiSolutions): Vielen Dank, Herr Henrichmann. Der Schritt wäre dann marginal. Dann würde es zwar noch die Meldepflichten etc. geben. In der Wirtschaft würden die, die jetzt schon reguliert sind, Finanzdienstleister, Telekommunikationsdienstleister, auf NIS-2 schulterzuckend schauen und sagen: Ja, das kriegen wir jetzt auch noch hin. Also alles, was an Kosten durch NIS-2 aufgebürdet wird, sind eigentlich Kosten, die zu 90 Prozent durch UP Bund angefallen und damit erledigt worden sind.

Ich will noch einmal auf Frau Griebsch eingehen. Auch ich stimme ihr zu, idealerweise wären die Kommunen mit dabei – das ist die kritischste Infrastruktur, die der Bürger sieht. Und das hat dann auch was mit Staatsversagen – sichtbar – für die Bürger zu tun, wenn man ein paar Monate lang kein Auto mehr anmelden kann, kein Unternehmen, etc. Gut, das werden wir aber da nicht mehr hineinbekommen. Aber ohne die Einbindung der nachgelagerten Behörden sollte dieses Gesetz nicht über den Tisch gehen. Machen wir es ganz konkret. Ich muss, wie schon erwähnt, eine Grundschutzzertifizierung haben, damit ich in nachgelagerten Behörden wenigstens Verschlusssachen - Nur für den Dienstgebrauch (VS-NfD) Eingestuftes ansehen kann. Die nachgelagerte Behörde kann aber Geheim- und Verschlusssachen ohne das ansehen. Da sieht man schon, dass es schizophren wird. Nun, Netze des Bundes: Vorne haben wir eine Stahltür, hinten haben wir ein Flatterband. Wie soll das in Zukunft funktionieren, dass die involvierten Behörden miteinander kommunizieren? „Nachgelagert“ heißt nicht nachrangig von Interesse für Geheimdienste. Wir hatten im letzten Jahr den Fall des Bundesamtes für Kartographie und Geodäsie, die von chinesischen Nachrichtendiensten ausspioniert worden sind, wo man festgestellt hat, dass das wahnsinnig viele spannende Daten über kritische Infrastrukturen waren. Die einzige gute Nachricht, die ich dann hätte: Wir können vielleicht die Anzahl der Drohnenflüge reduzieren, wenn wir das Scheunentor offenlassen. Dann können sie sich konzentriert die Daten abholen und müssen nicht mehr mit Drohnen umherfliegen. Es ist einfach ein absolutes Unding, dass wir auf dieser Ebene die nachgeordneten Behörden nicht mit hineinnehmen, weil das zu Tausenden Problemen führt. Das ganze Thema muss dann, und zwar mit einem starken CISO und deswegen koordiniert auf einer gemeinsamen Basis und mit effizienteren Wegen, umgesetzt werden. Und dann ist es eben auch kein so wahnsinnig unvorstellbarer Schritt mehr. Dank der Grünen ist im Sondervermögen Cyber-Sicherheit genannt – dafür kann man es doch verwenden!

SV **Felix Kuhlenkamp** (Bitkom): Auch von meiner Seite danke für die Frage. Ich kann mich der Argumentation und der Analyse von Timo Kob grundsätzlich komplett anschließen. Ich würde mich kurz auf das Stimmungsbild in der Wirtschaft konzentrieren: Als größter Digitalverband in Deutschland stehen wir im Austausch mit Konzernen, Mittelstand, Kleinstunternehmen, Startups, und eigentlich ist das Schöne in der Cyber-Sicherheit, dass man mit Wirtschaft und Staat an einem

gemeinsamen Ziel arbeitet, nämlich der Schutz und die Resilienz von digitalen Infrastrukturen. Doch bei der geplanten Ausnahme der nachgeordneten Bundesbehörden fällt es mir ehrlich gesagt zunehmend schwer, diese gemeinsame Linie zu erkennen und auch zu erklären. In Gesprächen mit den Unternehmen wird deutlich, dass es für diese Ausnahmen absolut kein Verständnis gibt. Diejenigen, die sich über Jahre lang hinweg mit NIS-2 auseinandergesetzt haben, reagieren frustriert, wenn man mit ihnen darüber spricht. Die Unternehmen oder die Personen, die sich nicht täglich mit NIS-2 beschäftigen, fallen aus allen Wolken, wenn man ihnen die Ausnahmen im Detail erklärt. Das Vorhaben irritiert die Wirtschaft und es untergräbt auch die Glaubwürdigkeit und Akzeptanz dieser Regulierung. Wenn man sich einmal einzelne Sektoren heraussucht – ich habe im Vorfeld noch einmal in den BSI-Lagebericht hineingeschaut – da werden die KRITIS-Sektoren nach Reifegraden sortiert, die Wasserwirtschaft ist zum Beispiel sehr gut etabliert, da frage ich mich, wie soll man diesen Unternehmen erklären, dass die Verwaltung nicht in der Lage sein soll, ähnliche Standards umzusetzen? Und im Gesundheitssektor liegen die Reifegrade vieler Einrichtungen erst auf Stufe zwei von fünf. Wie soll man dort Fortschritt abverlangen, wenn die Verwaltung selbst kein Vorbild ist? Auch das Argument von hohen Umsetzungskosten greift meiner Meinung nach zu kurz. Timo Kob hat das schon richtig analysiert. Wenn UP Bund richtig umgesetzt wäre, wären die Kosten nicht so hoch. Und wenn es erst mal zu einem erfolgreichen Cyber-Angriff kommt, dann haben wir deutlich höhere Kosten, als jetzt im Vorfeld zu investieren. Daher bleibt mir nur erneut zu sagen, dass alle Behörden und Einrichtungen des Bundes den gleichen Pflichten wie Unternehmen unterliegen sollten.

Amt. Vors. **Josef Oster** (CDU/CSU): Vielen Dank. Wir fahren fort mit der AfD-Fraktion.

Abg. **Steffen Janich** (AfD): Vielen Dank. Meine erste Frage geht an Herrn Kob. Eigentlich wollte ich auf Ihren Einleitungssatz eingehen, die unsägliche Ausnahme der nachfolgenden Behörden. Das hat der Kollege von der CDU jetzt schon abgearbeitet. Insofern würde mich aber trotzdem interessieren: Gehen Sie davon aus, dass die Unternehmen in Deutschland aktuell überhaupt darauf vorbereitet sind, die Vorgaben von NIS-2 so umzusetzen? Und wo sehen Sie, wenn die Unternehmen darauf eingehen, die größten Probleme, wo könnte es am meisten hapern?

Und meine zweite Frage geht an Herrn Kuhlenkamp. Ein Jahr Verspätung, das ist quasi die gleiche Frage, wir haben ein Jahr Verspätung, Sie haben von Zeitdruck, Strafzahlungen und mangelnder Wettbewerbsfähigkeit gesprochen. Vielleicht können Sie uns das noch einmal erläutern. Wie wirkt sich das jetzt auf die Unternehmen aus? Sind wir ein Jahr zu spät und haben sich dort schon entsprechende Schäden in der Wirtschaft bemerkbar gemacht? Oder haben wir jetzt mehr Zeit, um dort entsprechend aktuell jetzt ordentlich einzusteigen? Vielen Dank.

Amt. Vors. **Josef Oster** (CDU/CSU): Eine Frage an Herrn Kob und eine an Herrn Kuhlenkamp. In dieser Reihenfolge, bitte.

SV **Prof. Timo Kob** (HiSolutions): Es ist sicherlich nicht so, dass es nichts zu tun gibt oder dass es, wie es in Ihrer Fraktion heißt, nur ein „Fliegenschiss“ wäre. Aber was NIS-2 fordert, sind keine Dinge, die irgendwo vom Mond stammen und die nicht jedes Unternehmen selbst sowieso umsetzen kann, nichts von „Jetzt bauen wir da mal ein Bürokratiemonster auf“, sondern selbst wenn ich nicht davon betroffen wäre, würde ich genau die gleichen Dinge umsetzen, um überhaupt sicher zu sein. Daher mag es auf den ersten Blick unangenehm sein, vielleicht hätte ich mir auch gewünscht, dass die Grenzen, die auf EU-Ebene sind, ein bisschen höher angesetzt wären, um ein paar kleinere Unternehmen vor Bürokratie zu schützen. Aber aus der gleichen Sicht, die Frau Griebsch hat, dem Incident Response: Wir kennen auch Unternehmen mit 50 Mitarbeitern, die insolvent gehen, weil die Daten unverschlüsselt sind. Und um die davor zu schützen, muss man sie eben manchmal zu ihrem Glück zwingen. Manche haben da viel zu tun, für andere ist der Weg einfacher. Aber sie müssten ihn auch ohne Gesetz gehen, einfach, um nicht in Zukunft gefährdet zu sein.

SV **Felix Kuhlenkamp** (Bitkom): Zu der zweiten Frage. Wir sagen den Mitgliedsunternehmen und Unternehmen, mit denen wir im Dialog stehen: Grundsätzlich sollten sich natürlich alle Unternehmen längst mit NIS-2 befasst haben und sich im Idealfall darauf vorbereitet haben. In vielen Fällen trifft das zu, aber nicht immer. Man muss sagen, durch die Verzögerung im letzten Jahr haben wir

ein bisschen Momentum verloren. In meiner Wahrnehmung ist es durchaus so, dass damals große Aufmerksamkeit auf dem Thema lag, die dann ein bisschen verloren gegangen ist. Aber jetzt ist die Lage nun einmal, wie sie ist. Ich würde sagen, wenn wir uns jetzt darauf konzentrieren, NIS-2 eins zu eins umzusetzen und uns auf die wesentlichen Punkte konzentrieren, dann können wir nichtsdestotrotz gut aus der Sache rauskommen. Ein weiterer Punkt, der natürlich auch noch besprochen werden müsste, ist dieser Vergleich zu anderen europäischen Mitgliedstaaten. Gerade international tätige Unternehmen müssen gleiche Marktbedingungen im Binnenmarkt haben. Von daher ist es wichtig, darauf zu achten, dass die Maßnahmen überall gleich sind, auch in Deutschland.

Amt. Vors. **Josef Oster** (CDU/CSU): Vielen Dank. Wir fahren fort mit der SPD-Fraktion. Herr Schätzl.

Abg. **Johannes Schätzl** (SPD): Danke, Herr Vorsitzender. Ich würde die Zeit wieder splitten. Eine Frage an Herrn Professor Schröder. Ich blicke auf das BSI. Die Frage ist, welche weiteren Befugnisse sehen Sie beim BSI auch angesichts der gegenwärtigen Sicherheitslage als notwendig? Beispielsweise blicke ich in den § 15 BSIG, also die Erweiterung der Scan-Befugnis oder in den § 16 BSIG, wo wir die Herabsetzung der 100 000-Kunden-Grenze sehen. Die Frage ist also konkret, welche weiteren Befugnisse sehen Sie beim BSI als notwendig?

Abg. **Daniel Baldy** (SPD): Ich würde meine Frage an Herrn Professor Kob stellen. Das Thema ist eben schon angesprochen worden: Wie weit wissen Unternehmen der Wirtschaft eigentlich, dass sie betroffen sind? Da war ein Punkt, den wir letztes Jahr ganz oft angesprochen haben, wie wir es schaffen, die Unternehmen auch zu informieren. Sehen Sie da den Gesetzentwurf jetzt als final und perfekt, um die gesamte Wirtschaft zu erreichen, oder sehen Sie da auch noch Nachsteuerungsbedarf?

Amt. Vors. **Josef Oster** (CDU/CSU): Vielen Dank. Dann in dieser Reihenfolge. Herr Schröder und dann Herr Kob.

SV **Prof. Dr. Meinhard Schröder** (Universität Passau): Vielen Dank. Die NIS-2-Richtlinie verfolgt ein bisschen das Ziel der regulierten Selbstregulierung. Man möchte eigentlich nicht so unmittelbar mit Befugnissen agieren, sondern lieber, Sie hatten es eben schon gesagt, die Unternehmen zu etwas bringen, was sie vielleicht vernünftigerweise sowieso machen würden. Ja, was könnte man machen? Der § 15 BSIG sieht diese Scan-Befugnisse im Hinblick auf bekannte Schwachstellen vor, was natürlich nicht darin enthalten ist, sind Zero-Day-Exploits. Sollte das BSI das machen? Es kommt natürlich dann schnell in die Nähe eines verlängerten Arms der Nachrichtendienste und ich weiß nicht, ob das eine gute Situation für diese Behörde ist, die ja doch eigentlich eher für IT-Sicherheit da ist. Da kommen wir sehr schnell wieder zu dem anderen Punkt, was eben nicht hinreichend geregelt ist: Diese Rollenkonflikte und wie man mit Schwachstellen umgeht, die man dabei ja dann möglicherweise entdeckt. Von daher wäre ich dabei eher skeptisch. Was den § 16 BSIG angeht, da würde ich tatsächlich dafür plädieren, diese Grenze herabzusetzen. Das ist so ein bisschen wie das, was wir vorhin auch schon diskutiert haben. Es darf bei dieser Geringfügigkeits-Ausnahme nicht darauf ankommen, dass man irgendeine quantitative Betrachtung zugrunde legt, sondern es muss um die Kritikalität des Dienstes gehen. Wenn ich jetzt zum Beispiel an einen kleinen Stadtnetzbetreiber im Telekommunikationsbereich denke, wir haben in Passau Telepark und es gibt überhaupt nur 50 000 Einwohner in Passau, also bedeutend weniger Anschlüsse, ein Teil davon ist bei der Telekom. Und trotzdem: Wenn Telepark ausfallen würde, wäre das sehr schlimm. Die ganze Stadtverwaltung läuft, soweit ich weiß, über Telepark. Einen Ausfall durch einen Angriff dort will man nicht haben. Diese Hunderttausender-Grenze scheint mir in dem Zusammenhang nicht sinnvoll, man sollte wirklich auf Kritikalität abstellen!

SV **Prof. Timo Kob** (HiSolutions): Vielen Dank für die Frage. Darüber habe ich auch viel nachgedacht. Aber ich bin an dem Punkt relativ pragmatisch: Am Gesetz *muss* geändert werden, sozusagen „Karthago muss zerstört werden“, die nachgeordneten Behörden sind einzubeziehen, die Rolle des CISOs muss konkretisiert werden und danach würde ich Schluss machen. Ja, ich würde mir mehr wünschen an dem Punkt. Ich finde auch, am § 41 BSIG kann man und muss man viel tun. Richtige Ansätze sind drin, aber aktuell wäre mein Punkt lieber wirklich die Eins-zu-eins-Umsetzung so schnell wie möglich durch die Tür zu bekommen, und andere Themen gegebenenfalls – und da kom-

men ja noch Themen wie CRA, wie KRITIS-Dach-Gesetz – darüber zeitnah zu regeln, weil ich glaube, das Verständnis der Wirtschaft, dass sie was tun müssen, ist durchaus vorhanden. Ich sehe aber auch den aktuellen Stillstand – das ist nicht nötig! Die Unternehmen könnten sofort loslegen. Da ändert sich nichts mehr. Trotzdem aus irgendwelchen psychologischen Faktoren beginnen nur die wirklich großen und die, die eigentlich schon gut aufgestellt sind und die Kleinen beginnen eben noch gar nicht. Um da diesen Startschuss einfach sichtbar hineinzubekommen, mit diversen Unfertigkeiten und Unschönheiten, da sind wir alle sehr deutsch und versuchen noch die 110 Prozent und noch ein bisschen Gold-Plating hier und da – ich würde darauf verzichten und mich wirklich eins zu eins auf das konzentrieren, was umgesetzt werden muss! Das so schnell wie möglich. Und alles das, was Konfliktpotenzial hat und nicht in der EU-Richtlinie explizit gefordert ist, muss noch geregelt werden, aber nicht in diesem Kontext. Daran sind wir vor einem Jahr gescheitert, zu viele Punkte links und rechts. Das Thema Schwachstellenmanagement ist auch sicherlich sehr wichtig, aber gegebenenfalls einfach nicht in diesem Gesetz. Wir müssen schnellstens loslegen und dann lieber mit 80 Prozent und die 20 Prozent danach regeln.

Amt. Vors. **Josef Oster** (CDU/CSU): Vielen Dank. Es geht weiter mit BÜNDNIS 90/DIE GRÜNEN. Frau Dillschneider.

Abg. **Jeanne Dillschneider** (BÜNDNIS 90/DIE GRÜNEN): Vielen Dank, Herr Vorsitzender. Ich habe zwei Fragen an Herrn Professor Kipker. Die erste Frage: Herr Kipker, Sie gehen in der Stellungnahme auf den Punkt der „vernachlässigbaren Geschäftstätigkeit“ ein, wo aus Ihrer Sicht eine Abweichung zu den Grundsätzen der NIS-2-Richtlinie gegeben ist. Inwieweit halten Sie diesen Rechtsbegriff der „vernachlässigbaren Geschäftstätigkeit“ für ein hinreichendes Kriterium, um festzustellen, wie relevant ein Dienst oder eine Tätigkeit mit Blick auf die Cybersicherheit zu beurteilen ist? Und sehen Sie da ein Problem in Hinsicht auf die mangelnde Bestimmtheit und auch die zweifelhafte EU-Rechtskonformität?

Und die zweite Frage bezieht sich auf die CER-Richtlinie. Das wurde eben schon mehrfach angesprochen, dass es natürlich sinnvoll gewesen wäre, dass die Bundesregierung ein echtes KRITIS-Dach-Gesetz vorlegt und hier auch einen Gleichklang schafft zwischen der CER-Richtlinie und dem Schutz durch die NIS-2-Richtlinie. Es ist außerdem klar, dass die physische Sicherheit in Zeiten von hybriden Angriffen, Spionage, Sabotage elementar wichtig ist. Können Sie noch einmal darlegen, warum es wichtig wäre, beide Richtlinien zusammen umzusetzen und hier Einheitlichkeit zu schaffen, und was notwendig wäre, um das mit Blick auch auf die Aufsichtsbehörden umzusetzen?

Amt. Vors. **Josef Oster** (CDU/CSU): Vielen Dank. Zwei Fragen an Sie, Herr Kipker. Bitte schön.

SV **Prof. Dr. Dennis-Kenji Kipker** (Universität Bremen): Vielen Dank für die Möglichkeit, dazu auch noch Stellung zu nehmen. Was wir eben sehen bei diesen „vernachlässigbaren Tätigkeiten“ – wir haben gerade viel über Gold-Plating gesprochen; ich glaube, das hier ist jetzt „Under-Plating“ – man versucht hier meiner Meinung nach ein unzureichend fundiertes und potenziell auch gefährliches Kriterium in die nationale NIS-2-Umsetzung aufzunehmen. Aus zwei Gründen, einmal technisch und einmal rechtlich argumentiert, denn das Kriterium, das wir hier haben, geht über die vorgesehenen Schwellenwerte hinaus, die durch die NIS-2-Richtlinien definiert werden, also Größe und Umsatz, und berücksichtigt diese tatsächliche kritische Abhängigkeit oder diese systemische Bedeutung, die NIS-2 adressiert, meiner Meinung nach nicht ausreichend. Das Hauptproblem liegt auch darin, dass die Relevanz eines Dienstes oder einer Tätigkeit für das Gesamtgefüge der Cybersicherheit eben nicht nur von der Größe und dem Umsatz eines Unternehmens abhängig ist. Wir haben schon öfter von diesem Impact-Based Approach gehört, dass man sich jetzt mehr und mehr auf die digitale Lieferkette stützt. Beispielsweise kann ein IT-Dienstleister, dessen Geschäftstätigkeit beispielsweise als „vernachlässigbar“ eingestuft wird, da er nur wenige Beschäftigte in dem Bereich zum Beispiel hat, dennoch einen hochkritischen Dienst darstellen, beispielsweise, wenn er für Krankenhäuser oder Stadtwerke tätig wird. Das könnte eine erhebliche Kettenreaktion auslösen. Das heißt, wenn wir diese Ausnahme hineinnehmen, würden wir diese ganzen Kaskadeneffekte, die die NIS-2-Richtlinie eigentlich adressieren will, aufnehmen.

Und zum anderen ist es so, dass die NIS-2-Richtlinie eindeutig die Kriterien für die Anwendbarkeit festlegt. Das hat man gerade so gemacht, weil es in der Vergangenheit mit der NIS-1-Richtlinie nicht

der Fall gewesen ist und die Mitgliedstaaten damit auch sehr unterschiedlich umgegangen sind. Man hat hier eben gesagt, man will ein gemeinsames, einheitlich hohes Cyber-Sicherheitsniveau in der EU realisieren – und das wird dadurch nicht realisiert. Und es schafft gleichzeitig auch erhebliche Rechtsunsicherheit bei den Unternehmen, weil sie aus dem Gesetzestext nicht klar entnehmen können, was konkret „vernachlässigbar“ bedeutet. Die Frage wurde mir an der Stelle auch schon sehr, sehr oft gestellt. Deswegen meine Empfehlung, diesen Passus hier zu streichen.

Der zweite Punkt befasst sich natürlich mit einer sehr relevanten Fragestellung, nämlich diesen sogenannten hybriden Bedrohungen. Das ist jetzt auch schon durch die anderen Sachverständigen mehrfach angeklungen. Das heißt, Cyber-Security ist von gestern. Wir sprechen heutzutage von digitaler Resilienz. Wir reden nicht nur über Cyber-Angriffe, wir reden auch über Desinformation, wir reden über physische Sabotage, Störungen der Lieferkette. Und wenn wir sagen, die Europäische Union hat im Gleichklang CER und NIS-2 auf den Weg gebracht, dann muss sich diese Komplementarität dieser Bedrohungslage letzten Endes auch in der nationalen Gesetzgebung irgendwo spiegeln. Und das kann man einerseits dadurch forcieren, indem beispielsweise auch schon ein One-Stop-Shop vorgesehen ist. Das heißt, wir haben eine zentrale Anlaufstelle, eine Koordinierungsplattform und die Unternehmen, die Eilmeldungen vornehmen, müssen dann auch ein Feedback bekommen.

Was wir auch dringend benötigen, ist das einheitliche Lagebild. Darüber spricht Frau Plattner schon seit Längerem, ich glaube, sie nennt das „Cyber-Wetterbericht“. Das heißt, wir müssen über alle Bedrohungsvektoren hinweg in der Lage sein, diese Anforderungen zu analysieren. Wir müssen Melde- und Registrierungspflichten erleichtern. Wir müssen in der behördenübergreifenden Koordination und Prävention dieser ganzen Herausforderungen besser werden. Weil letzten Endes, wie ich schon gesagt habe, geht es nicht nur um Cybersicherheit, sondern um die Steuerung der gesamtstaatlichen Sicherheitsvorsorge. Und da haben wir natürlich das BBK auf der einen Seite, als nationale Resilienzbehörde im physischen Bereich, das BSI im Cyber-Bereich. Das wird natürlich so bleiben, aber der Schlüssel liegt meiner Meinung nach einfach in einer viel, viel institutionalisierteren, engeren Zusammenarbeit und vielleicht auch, und das ist bislang noch nicht so richtig deutlich geworden, einer Kooperation mit sektorspezifischen Aufsichtsbehörden. Was ist mit einer Bundesnetzagentur? Was ist beispielsweise mit dem Eisenbahnbundesamt? Und die müssen eben natürlich für eine einheitliche Governance auch in solche Resilienzpläne viel, viel stärker als bislang einbezogen werden. Danke.

Amt. Vors. **Josef Oster** (CDU/CSU): Vielen Dank. Frau Vogtschmidt für die Linke.

Abg. **Donata Vogtschmidt** (Die Linke): Vielen Dank. Ich würde noch einmal an meiner zweiten Frage aus der ersten Fragerunde anschließen. Und zwar über den Zeitplan des Gesetzentwurfes, weil ein anderer Kollege von den Sachverständigen meinte, dass die Kommunen natürlich schon sehr wichtig sind, aber dass wir die jetzt nicht mehr hineinbekommen. Sehen Sie das auch so? Oder wären vielleicht die rechtlichen Hürden diesbezüglich gar nicht so groß, beziehungsweise die Frage, die ich mir dann auch so stelle, ist, ob es nicht vielleicht auch hinsichtlich einer Etablierung einheitlicher Standards und Prozesse für die IT-Sicherheit dabei sogar massive Erleichterungen geben könnte.

Und die zweite Frage, die ich da noch hätte, wäre: Halten Sie die NIS-2-Anforderungen, dass zuständige Stellen für die IT-Sicherheit unparteiisch und auch frei von unzulässiger Einflussnahme sein sollten, bisher ausreichend abgebildet? Beziehungsweise was wäre das Minimum, was hier im BSI-Gesetz geändert werden sollte, auch mit Blick auf mögliche Weisungen, die nicht im Sinne der IT-Sicherheit sind. Vielen Dank.

Amt. Vors. **Josef Oster** (CDU/CSU): Ich konnte jetzt nur der Blickrichtung entnehmen, dass Sie Frau Griebsch meinen. Ist das so? Bitte schön, Frau Griebsch.

SVe **Sabine Griebsch** (GovThings): Ich habe mich schon seelisch und moralisch vorbereitet. Vielen Dank. Was den Zeitplan betrifft: Was Professor Kob sagt, das ist natürlich knapp. Auf der anderen Seite ist die Frage, wie wichtig ist mir das? Auf der einen Seite will ich die Kommunen drin haben und auf der anderen Seite, was hält uns davon ab, die Kommunen und die Länder nicht drin zu haben? Das heißt, ich finde es immens wichtig, dies in das Gesetz mit aufzunehmen und es tatsächlich umzusetzen und hier für Klarheit zu sorgen. Natür-

lich heißt es auch, dass Unternehmen 21 Monate Zeit hatten, sich darauf vorzubereiten. Kommunen haben das nicht. Das ist mit einer auskömmlichen Anpassung der Fristen an Kommunen durchaus abbildbar. Auf der anderen Seite ist es natürlich wichtig, dass ich in einer Situation überhaupt keine Kompromisse eingehe, nämlich wann Kommunen ins Lagebild Meldungen geben sollten. Und zwar sollte das definitiv sofort geschehen. Deswegen ist es in meiner Betrachtung unfassbar wichtig, Kommunen sofort mit aufzunehmen, um reaktionsfähig zu sein, um überhaupt ein umfassendes Lagebild zu haben. Jetzt muss ich mich ganz kurz an die zweite Frage erinnern.

Abg. **Donata Vogtschmidt** (Die Linke): Es war die Frage, ob die zuständigen Stellen für die IT-Sicherheit, dass die unparteiisch und frei von unzulässiger Einflussnahme sein sollen, ob die bisher im NIS-2-Gesetz ausreichend abgebildet sind und was das Minimum wäre, was im BSI-Gesetz geändert werden sollte?

SVe **Sabine Griebsch** (GovThings): In meiner Betrachtung ist es tatsächlich nicht so. Wenn ich jetzt an die Stelle des CISO Bund denke, dann ist es in meiner Bewertung so, dass der dringend eingerichtet werden muss. Er muss ein Vetorecht haben, er muss ein Weisungsrecht gegenüber den Ressorts haben. Aktuell fehlen die konkreten Verpflichtungen. Es fehlt die konkrete Ausgestaltung dieser Fläche und die gesetzliche Verankerung der Unabhängigkeit des CISO. Das heißt, mit diesen klaren Befugnissen, die sich natürlich auch auf die kommunale Ebene auswirken könnten, wenn ich jetzt wieder auf meiner Scholle bleibe, dann ist es notwendig, das tatsächlich dort mit hineinzuschreiben. Wie gesagt, bei den Weisungsbefugnissen, da ist es unheimlich wichtig, dass wir einheitliche Sicherheitsvorgaben haben und dass die Steuerungs- und Eskalationskompetenzen hier dabei sind. Ich habe mir in meiner Vorbereitung tatsächlich notiert, dass das BSI natürlich unabhängig sein sollte. Das heißt, um hier ein einheitliches Cyber-Sicherheitsniveau zu haben und hier auf der anderen Seite auch eine glaubwürdige Stelle zu haben, die unabhängig agiert – das sehe ich absolut bei dem BSI. Ich hoffe, ich habe das ausführlich beantwortet. Wenn nicht, gern noch einmal eine Nachfrage in der nächsten Runde gegebenenfalls.

Amt. Vors. **Josef Oster** (CDU/CSU): Vielen Dank. Wir sind mit der zweiten Fragerunde durch und liegen gut in der Zeit. Ich würde dann in die dritte Runde überleiten. Wir gehen in der üblichen Reihenfolge weiter vor. Die CDU/CSU-Fraktion hat das Wort, Herr Kollege Henrichmann.

Abg. **Marc Henrichmann** (CDU/CSU): Vielen Dank. Ich würde gern mit einer Frage an Herrn Gehringer und Herrn Kuhlenkamp in die dritte Runde gehen. Und zwar noch einmal zu dem Thema „kritische Komponenten“. Wir haben heute Morgen die Anhörung der Präsidenten der Nachrichtendienste gehabt, die die Bedrohungslage in Deutschland und Europa noch einmal geschildert haben, zu hybriden Bedrohungen, hybridem Krieg bis hin zur Manipulation und auch Terrorismus und alles, was damit verbunden ist. Und deswegen ist sozusagen dieser Punkt „kritische Komponenten“ auch einer, dem man sich nach meinem Dafürhalten unbedingt widmen muss. Jetzt kann man natürlich durch verschiedene Brillen darauf blicken und wir kennen auch die Diskussion, die im letzten Jahr, wenn man so will, NIS-2 zum Explodieren gebracht hat, kurz vor knapp und ohne Anhörung. Aber die Frage ist halt wieder da. Ich denke, wir sind uns einig, dass ein Staat in Zeiten höchster Bedrohung reagieren können muss, indem er kritische Komponenten, die die nationale Sicherheit massiv gefährden, dann auch in letzter Konsequenz untersagt. Und deswegen die Frage dazu aktuell, Herr Kuhlenkamp, was die Wirtschaft betrifft: Wie ist da das Stimmungsbild? Wie sieht es auch mit alternativen Verfügbarkeiten aus? Und Herr Gehringer, die sicherheitspolitischen Argumente, die dafür sprächen, die hätte ich gern von Ihnen zusammengefasst. Danke.

Amt. Vors. **Josef Oster** (CDU/CSU): Vielen Dank, Herr Kollege. Herr Kuhlenkamp und dann Herr Gehringer.

SV **Felix Kuhlenkamp** (Bitkom): Alles klar, danke für die Frage. Die Diskussion um kritische Komponenten begleitet uns im Bitkom nun auch seit vielen Jahren. Sie wird lebhaft geführt innerhalb unserer Mitgliedschaft, weil es da zum Teil deutlich unterschiedliche Perspektiven gibt, auch auf die Punkte, die Sie angesprochen hatten. Wir hatten die Diskussion eben auch im vergangenen Dezember, als die Formulierungshilfen für das NIS-

2-Umsetzungsgesetz vorgelegt wurden. Damals herrschte vor allem in einem Punkt Einigkeit: Der Vorschlag kam damals völlig ohne Abstimmung mit den betroffenen Branchen. Ein Dialog fand nicht statt. Und die Änderungen waren auch losgelöst von der eigentlichen Diskussion, die wir um NIS-2 geführt haben und hat die ganze Sache deutlich verkompliziert. Genau an diesem Punkt stehen wir aus meiner Sicht wieder – die Zeit drängt. Wir haben ein Vertragsverletzungsverfahren und es wird über Eingriffe in die Wirtschaft gesprochen, ohne dass ein konkreter Entwurf vorliegt, über den wir diskutieren können. Daher fällt es mir manchmal ein bisschen schwer, dafür qualifiziert Stellung zu nehmen. Dabei hätten wir eigentlich Beispiele, wie es mit dem Dialog besser funktioniert, zum Beispiel beim öffentlich-rechtlichen Vertrag zwischen den Mobilnetzbetreibern und der Bundesregierung aus dem Jahr 2024. Nach meinem jetzigen Kenntnisstand liegt eigentlich wieder derselbe Wortlaut wie im Dezember letzten Jahres auf dem Tisch. Sollte das stimmen, gibt es erhebliche Bedenken gegenüber der Idee, dass das BMI künftig nur im Benehmen mit den Fachministerien die Verwendung kritischer Komponenten untersagen könnte. Das würde bedeuten, dass die fachliche Expertise der Aufsichtsbehörden, etwa des BSI oder der Bundesnetzagentur außen vor bleibt. Das BMI sollte auch weiterhin per Rechtsverordnung kritische Funktionen und Komponenten festlegen können, allerdings im Einvernehmen mit Fachministerien unter Einbeziehung der zuständigen Behörden. Es bleiben außerdem andere zentrale Fragen offen, wie nach den Kosten, wenn die verbaute Technik zurückgebaut werden muss. Wichtig ist uns vor allem, dass Verbände, Unternehmen und ExpertInnen kontinuierlich eingebunden sind. Wir plädieren deswegen dafür, die Diskussion um kritische Komponenten von der Umsetzung von NIS-2 zu trennen, sonst verlieren wir weiter Zeit und erzeugen zusätzliche Unsicherheit. Wir stehen dann aber gern bereit für einen sicherheitspolitischen Dialog in einem geordneten Verfahren.

Amt. Vors. **Josef Oster** (CDU/CSU): Vielen Dank. Herr Gehringer.

SV **Ferdinand Gehringer** (Konrad-Adenauer-Stiftung): Daran anschließend: „Zeit“ war ein gutes Stichwort. Wenn es in der Kürze der Zeit gelingt, die Bedenken aus der Wirtschaft hinreichend zu berücksichtigen, dann erfordern nicht nur die sicherheitspolitische Lage und die hybriden Angriffe die dringende Untersagungsmöglichkeit bei kritischen Komponenten, sondern auch die Tatsache, dass Kritis ganz gezielt als Zielscheibe verwendet wird und dass mit den Abhängigkeiten als Druckmittel gespielt wird. Es gibt da sicherheitspolitisch keine zwei Meinungen, dass das zwingend notwendig sein muss. Dabei sollte man allerdings dringend auch einige Zwecke, Interessen, die teilweise auch gegenläufig sind, berücksichtigen. Wir haben schon von Herrn Kuhlenkamp gehört, dass es immer große Bedenken hinsichtlich der Bürokratie gibt, dass es Bedenken hinsichtlich der Planungssicherheit, Wettbewerbsnachteilen, der praktischen Umsetzbarkeit gibt, dass es aber vor allen Dingen auch eine Vertrauensfrage bei dem Umgang mit kritischen Komponenten zwischen den zuständigen Ministerien und den Betreibern aus der Privatwirtschaft ist. Wenn es gelingt, in einem transparenten Verfahren dieses gegenseitige Vertrauen zwischen der Privatwirtschaft und dem Ministerium, was dann diese Letztentscheidungskompetenz hat, zu klären und ein rechtssicheres und planungsfestes, ein transparentes Verfahren einzuführen mit objektiv klaren Kriterien – der bisherige Entwurf ist noch zu unscharf in dem Zusammenhang –, die die technischen Aspekte, die die organisatorischen Aspekte und die geopolitischen Aspekte alle berücksichtigen, um dann in der summarischen Prüfung eine Entscheidung zuzulassen, dann gibt es die Möglichkeit, über den § 41 BSIG zu sprechen und über eine Verschärfung nachzudenken. Es muss aber klar sein, dass die Bürokratie, die bisher im § 41 BSIG umfasst ist, deutlich abgebaut werden muss.

Und der letzte Gedanke dazu: Die Vollzugsfähigkeit, die klang auch im letzten Moment an. Vielleicht könnte man überlegen, das wirklich im Einvernehmen mit dem Bundeskanzleramt zu machen. Wir sprechen hier von sicherheitspolitischen Erwägungen. Das sind hybride Angriffe gegen Deutschland. Kritis ist als Zielscheibe akut, wir haben das heute Morgen in der Anhörung gehört, sie ist im Blick anderer Nachrichtendienste und anderer Staaten. Und diese autoritären Staaten nutzen unsere Abhängigkeiten. Danke.

Amt. Vors. **Josef Oster** (CDU/CSU): Vielen Dank. Es geht weiter mit der AfD-Fraktion, Herr Janich.

Abg. **Steffen Janich** (AfD): Vielen Dank. Meine erste Frage geht an Herrn Professor Dr. Schröder.

Herr Professor Dr. Schröder, Sie hatten in Ihrem Eingangsstatement das mangelnde Schwachstellenmanagement angesprochen und Sie sprachen davon, dass bei Zufallstreffern noch eine Regelung gemacht werden sollte. Jetzt hatte Herr Professor Kob vorhin, wenn ich das richtig verstanden hatte, gesagt, dass ein Schwachstellenmanagement, ein Einpflegen in NIS-2-Richtlinien, nicht zulasten einer zeitlichen Verzögerung stattfinden soll. Wie würden Sie die Schwerpunkte setzen? Gehen Sie davon aus, dass es zeitnah eingebracht werden soll oder dass man das vielleicht auch im Nachgang mit einbringen könnte? Und wo setzen Sie konkret im Schwachstellenmanagement an, wovon sagen Sie, dass das auf jeden Fall mitgeregelt werden muss? Das wäre die erste Frage.

Die zweite Frage geht an Herrn Kuhlenkamp: Sie hatten in Ihrer Ausführung geschrieben, dass Unsicherheit besteht, welche Unternehmen betroffen sind, das heißt, die Abgrenzung gerade zu kleineren Unternehmen soll wohl noch nicht so richtig klar sein und es soll Unternehmen geben, die das nicht so richtig zuordnen können. Könnten Sie mir das noch einmal genau erklären? Vielen Dank.

Amt. Vors. **Josef Oster** (CDU/CSU): Danke schön. Zwei Fragen, eine an Herrn Professor Schröder und eine an Herrn Kuhlenkamp. In dieser Reihenfolge, bitte.

SV **Prof. Dr. Meinhard Schröder** (Universität Passau): Vielen Dank für die Frage. Das ist letztlich eine Frage über den Ablauf des parlamentarischen Verfahrens, die nur Sie beantworten können. Ich würde sagen, beide Punkte sind wichtig. In die Umsetzung der NIS-2-Richtlinie, das ist richtig, da gehört das nicht unmittelbar hinein. Und die ist überfällig, die hätte ja schon letztes Jahr umgesetzt müssen. Und wenn jetzt die Diskussion um den § 41 BSIG oder auch um andere Dinge, die noch zusätzlich drin sind, das Verfahren weiter verzögern würde, dann würde ich sagen, dann beschliessen Sie das eben in zwei unterschiedlichen Gesetzen. Trotzdem muss man sagen, dass auch das Schwachstellenmanagement ein wichtiges Thema ist. Das Bundesverfassungsgericht, Herr Kipker hat es schon erwähnt, hat bereits 2021 gesagt, dass da irgendetwas gemacht werden muss, dass da eine gesetzliche Regelung getroffen werden muss und die ist immer noch nicht da. Die muss nicht in diesem Gesetz sein. Aber so langsam könnte man doch damit anfangen, diesen Auftrag zu erfüllen!

SV **Felix Kuhlenkamp** (Bitkom): Die Fragen bzw. Schwierigkeiten bei der unklaren Betroffenheit beziehen sich bei unserer Stellungnahme hauptsächlich auf § 28 BSIG. Wie angesprochen, gibt es da die Ausnahmen für „vernachlässigbare Geschäftstätigkeiten“. Diese Ausnahmen sind aus unserer Sicht grundsätzlich richtig und die Idee ist gut. Es bedarf aber eben klarer Schwellwerte, um klar festmachen zu können, dass zum Beispiel, wenn man eine Ladesäule anbietet, an der sich die Mitarbeitenden ihr Elektroauto aufladen können, dass diese damit nicht auf einmal unter NIS-2 fällt, wenn es eigentlich ein Unternehmen ist, was eben nichts mit NIS-2 „am Hut“ hat. Und wenn es dann weiter um unklare Betroffenheiten geht im Bereich der Kleinstunternehmen, insbesondere also Unternehmen mit um die 50 Mitarbeitenden, dann ist das hauptsächlich, würde ich sagen, ein Awareness-Problem, ein Bewusstseinsproblem, weil die vielleicht nicht die Ressourcen haben, sich so viel mit so etwas auseinanderzusetzen. Da muss man ganz selbstkritisch sagen, dass das die Arbeit der Verbände ist, daran zu arbeiten. Und das tun wir. Gleichzeitig möchte ich da ein Kompliment ans BSI geben. Die haben eine wirklich gute Kommunikationsarbeit gemacht, um möglichst viele Unternehmen zu erreichen.

Amt. Vors. **Josef Oster** (CDU/CSU): Danke schön. Es geht weiter mit der SPD-Fraktion, Herr Schätzl.

Abg. **Johannes Schätzl** (SPD): Herzlichen Dank, Herr Vorsitzender. Eine Frage an Herrn Dr. Herpig, eine Frage an Herrn Kuhlenkamp. Herr Dr. Herpig, ich blicke auf § 14 BSIG und frage mich, ob es noch eine Anpassung beziehungsweise eine Klarstellung braucht, dass das BSI bei Kenntnis über Schwachstellen zwingend den Coordinated Vulnerability Disclosure (CVD)-Prozess starten muss, mit dem Ziel, die Schwachstellen zu schließen.

Die Frage an Herrn Kuhlenkamp bezieht sich noch einmal auf den § 41 BSIG. Sie haben nämlich zwei Teile angesprochen: Zum einen die Zeitkritikalität bei der Umsetzung und die Frage nach dem Benehmen oder Einvernehmen und das ein bisschen kombiniert zum Thema Zeitablauf. Ich gebe Ihnen recht, dass wir eine schnelle Umsetzung brauchen. Meine Frage für die Zeit wäre, ob es da maßgeblich ist, ob wir über diesen Punkt reden oder ob es nicht sein kann, dass man im parlamentarischen Verfahren auch schnell einen Punkt klären könnte und deswegen die zeitkritische Komponente

entfallen würde. Zweiter kleiner Teil dieser Frage bezieht sich auf das BSI. Jetzt haben Sie ja gesagt, dass das BSI auch die nachgelagerte Behörde ist, die die fachliche Einschätzung treffen kann. Die liegt aber im Geschäftsbereich des BMI. Deswegen noch einmal klar die Frage, warum müsste beispielsweise ein Verkehrsministerium sein Einvernehmen herstellen, wenn ja die Fachexpertise explizit durch das BSI beim BMI liegt?

Amt. Vors. **Josef Oster** (CDU/CSU): Danke schön für die Fragen. Die sind einmal an Herrn Dr. Herpig und an den Herrn Kuhlenkamp gerichtet. Herr Dr. Herpig, Sie haben als erster das Wort.

SV **Dr. Sven Herpig** (interface): Wunderbar. Vielen Dank. Auch zur Beantwortung von früheren Fragen zum Thema Schwachstellenmanagement. Wir haben natürlich eine Goldrandlösung zum Thema Schwachstellenmanagement, wo alle Behörden mit beteiligt sind. Wir selbst haben 2018 dazu einen Prozess vorgelegt. Das Innenministerium arbeitet seit vielen Jahren daran. Diese Goldrandlösung scheitert seit vielen Jahren an einer obersten Bundesbehörde. Daher werden wir die nicht durchkriegen in den nächsten Jahren vor allem nicht hier in der NIS-2-Regulierung. Es gibt aber ein weiteres Spektrum an Maßnahmen, die wir ergreifen können, um zumindest etwas zu tun, was die IT-Sicherheitsnutzung von Schwachstellen angeht im Vergleich zu Güterabwägungen für öffentliche Sicherheit oder andere Maßnahmen. Das wäre, dass wir in diesem Gesetz regeln, dass alle Kenntnisse über Schwachstellen, die das BSI erlangt, im Rahmen dieser gesetzlichen Regelung und im Rahmen seines Coordinated Vulnerability Disclosure Prozesses ausschließlich dafür genutzt werden können, diese Schwachstellen zu einer Mitigierung und/oder einer Behebung zuzuführen. Das bedeutet auch, dass es natürlich Schwachstellen geben kann, die nicht geschlossen werden können, weil es zum Beispiel den Maintainer von einer freien Software nicht mehr gibt, weil er oder sie nicht mehr in dem Projekt arbeitet, das ist dann eben hinzunehmen. Aber wenn wir so eine gesetzliche Regelung schaffen würden, wüssten wir zumindest, dass alle Sicherheitsforschenden, die sich an das BSI wenden, also diese Zufallsfälle, die vorhin genannt worden sind, als auch diejenigen, die Informationen über Schwachstellen, die im Rahmen dieses IT-Sicherheitsgesetzes gefunden, erhoben, was auch immer werden, nur genutzt werden, um IT-Systeme abzusichern. Gleichzeitig tendiere ich dazu, dass man den IT-Sicherheitsforschenden auch die Möglichkeit gibt, nicht nur anonym zu melden, sondern man auch bei pseudonymer oder bei Nennung von Schwachstellen unter normalen Namen den Zugang zu Rechtsschutz haben soll, das heißt, eine kostenlose Rechtsberatung zu erhalten, denn das Problem ist häufig nicht, dass IT-Sicherheitsforscher irgendwann verurteilt werden für eine Sicherheitsforschung, die zur IT-Sicherheit beigetragen hat, sondern weil erst einmal ihre Sachen beschlagnahmt werden, sie sich einen Rechtsanwalt suchen müssen und so weiter, also psychologische Probleme und Herausforderungen, die dadurch entstehen und die müssten wir entsprechend absichern, wenn wir wollen, dass die Schwachstellen zur IT-Sicherheit genutzt werden.

Amt. Vors. **Josef Oster** (CDU/CSU): Danke. Herr Kuhlenkamp.

SV **Felix Kuhlenkamp** (Bitkom): Danke, Herr Schätzl, für die Frage. Erst einmal zum Thema der Zeit: Wie Sie richtig gesagt haben, wir haben Zeitdruck. Es gibt ein Vertragsverletzungsverfahren, es gibt Unsicherheit in Unternehmen, insbesondere in denen, die international und europaweit agieren. Jetzt war die Frage von Ihnen, ob es nicht in der verbleibenden parlamentarischen Zeit möglich wäre, da zu einer Entscheidung zu kommen. Ich glaube, das hängt aus unserer Sicht auch maßgeblich davon ab, ob es denn möglich ist, in der restlichen Zeit einen ausreichenden tiefen Dialog mit der Wirtschaft zu führen, bei dem auch alle an einen Tisch kommen können und sich entsprechend einbringen können. Und das Gefühl haben wir bisher nicht. Und wir haben auch nicht das Gefühl, dass die Zeit ausreicht. Deswegen unsere Stellungnahmen in diese Richtung. Grundsätzlich, wenn Zeit da ist, dann nehmen wir diesen Prozess gern wahr und bringen uns entsprechend ein. Wir sehen einfach den Punkt, dass zum Beispiel beim Cyber Resilience Act noch kein Vertragsverletzungsverfahren läuft. Da ist der Zeitdruck nicht so hoch. Da könnte man sich in Ruhe hinsetzen und über diese Dinge diskutieren.

Zum Thema der Fachexpertise. Sie hatten das BSI als nachgelagerte Behörde des BMI genannt. Wie gesagt, aus unserer Sicht gibt es da auch insbesondere noch die Bundesnetzagentur. Wenn wir jetzt vom Beispiel vom Verkehrsministerium ausgehen, man kann im Detail darüber reden, welche Mini-

sterien in die Entscheidung einbezogen sind, aber beim Beispiel Verkehrsministerium denke ich mir, wenn die kritische Komponente den Verkehrssektor betrifft, dann sollten die schon einbezogen sein. Wenn ich zum Beispiel an autonom fahrende Autos denke und welche Komponenten da so verwendet werden. Wie gesagt, uns geht es darum, darüber diskutieren und uns einbringen zu können und auch irgendwie eine Grundlage zu haben, auf die wir uns beziehen können. Die haben wir aktuell nicht. Daher würden wir für eine Verlagerung plädieren.

Amt. Vors. **Josef Oster** (CDU/CSU): Danke schön. Gibt es bei den Grünen weitere Fragen? Ich sehe, das ist der Fall. Herr Dr. von Notz.

Abg. **Dr. Konstantin von Notz** (BÜNDNIS 90/DIE GRÜNEN): Vielen Dank, Herr Vorsitzender. Herr Kipker, ich will noch einmal auf das BSI zu sprechen kommen, will aber vorher noch einmal für die Runde allgemein sagen: Wenn man sich die Anhörung zu dem Entwurf der Ampel zu diesem Bereich anguckt und heute noch einmal die Anhörung, das ist wirklich, als wäre man in der Zeitschlaufe gefangen! Das ist so krass. Und bei „Täglich grüßt das Murmeltier“, der Bill Murray, ja, der hat ja viel Zeit. Aber angesichts der Sicherheitslage, dass wir uns das als drittgrößte Wirtschaftsnation der Welt leisten, das ist so verrückt! Deswegen finde ich das zum Verzweifeln!

Aber ich will noch einmal zum BSI fragen, Herr Kipker: Wie schauen Sie auf diese Frage der Abhängigkeit oder Teilunabhängigkeit, die für das BSI diskutiert wird, um die Vertrauensfragen, die angesprochen wurden, aufzulösen?

Und dann vielleicht, Herr Gehringer, die Anhörung heute Morgen bei den Nachrichtendiensten, in der eine ganze Reihe von Kollegen waren, die hier eben auch noch sind, die Frage, ob nicht eigentlich das BSI oder die Bundes-CISO an den Tisch des Nationalen Sicherheitsrats gehört? Wenn man sich anguckt, worüber wir reden und dann die Rolle des Nationalen Sicherheitsrats sieht, dann ist das meiner Ansicht nach zwingend, dass die da einen Platz am Tisch bekommen. Herzlichen Dank.

Amt. Vors. **Josef Oster** (CDU/CSU): Zwei Fragen. Einmal an Herrn Professor Kipker und dann an Herrn Gehringer. Herr Kipker, bitte.

SV **Prof. Dr. Dennis-Kenji Kipker** (Universität Bremen): Vielen Dank für die Frage. Wir haben seit Jahren über die Unabhängigkeit des BSI gesprochen, mit der AG BSI verschiedene Lösungsansätze erarbeitet. Ich glaube, diese Frage der Unabhängigkeit, die ist an mehreren Stellen schon angeklungen, das betrifft nicht nur die staatliche Frage, die Frage im institutionellen Gefüge, sondern auch, wie mit dem Thema Schwachstellen umgegangen wird. Es geht bei dem Thema Cybersicherheit, auch viel um das Thema Public-private-Partnerships. Da hört man es von Unternehmen immer wieder: Was passiert eigentlich mit meinen sensiblen Daten, wenn ich sie zum Beispiel an das BSI melde? Wird das irgendwo weitergegeben? Wir müssen auf jeden Fall diese Unsicherheit herausnehmen, weil sonst schwächen wir die Cybersicherheit in Deutschland nachhaltig. Die Wirksamkeit der IT-Sicherheit nicht nur für Private, was ich gerade angesprochen habe, sondern auch in der Bundesverwaltung wird letztendlich maßgeblich durch das Zusammenspiel eines unabhängigen BSI und letzten Endes auch eines starken CISO Bund bestimmt. Beide können, glaube ich, sehr viele Synergien schaffen, die wir bislang noch nicht ausreichend ausgegraben haben. Das BSI hat eben die Aufgabe, und deswegen fand ich auch die Kritik am Anfang sehr relevant, die im Hinblick auf § 1 BSIG geäußert wurde, dass es als technische Fachbehörde seine Aufgaben gegenüber allen Arten von Institutionen auf technisch-fachlicher Basis wahrnimmt. Deswegen erschließt es sich nicht, warum dieser § 1 BSIG, das hatte ich auch schon in der letzten Anhörung im November letzten Jahres angemerkt, nicht entsprechend glattgezogen wird und gesagt wird, es ist eine Fachbehörde für alle. Und das BSI ist eine zentrale technische Instanz, die sicherstellt, dass alle Behörden auf dem neuesten Stand der Technik geschützt werden, indem es den IT-Grundschutz entwickelt, kontinuierlich fortschreibt, als Fachexperte auch berät und die Sicherheitslage analysiert. Wir sehen andererseits aber auch, dass der CISO Bund, und da möchte ich vielleicht auch diese Frage etwas erweitern, unerlässlich für die ganzen Fragen um Koordination, Steuerung, Sicherstellung der Umsetzung ist. Ich glaube, es geht insgesamt darum, dass wir sagen: Wie können wir durch eine Unabhängigkeitsstellung des BSI eine Informationssicherheitskultur im Bund etablieren, die wir bislang eben nicht haben? Danke.

Amt. Vors. **Josef Oster** (CDU/CSU): Danke. Herr Gehringer.

SV **Ferdinand Gehringer** (Konrad-Adenauer-Stiftung): Ich habe vorhin schon in meinen Ausführungen erwähnt, dass idealerweise der CISO Bund die Federführung für die nationalen Cyber-Krisen hätte oder haben sollte. Wenn es uns gelingt, dass der Bundes-CISO, der idealerweise beim BSI, aber nicht in der Position der Präsidentin verortet wird, sondern in einer vergleichbaren Position, beispielsweise beim Vizepräsidenten, verankert ist, wenn es uns gelingt, diese Rolle sehr stark mit starken Durchgriffsrechten, wie ich sie vorhin ausgeführt habe, mit starken Befugnissen, Weisungsrechten, aber auch mit Berichtspflichten, siehe Bundesrechnungshof, siehe aber auch gegenüber dem Parlament, auszustatten, wenn er diese starke Rolle einnehmen soll, dann würde es voll und ganz Sinn ergeben, ihn auch als Teil des Nationalen Sicherheitsrates aufzunehmen, um vor allen Dingen dem Thema der Informationssicherheit in der Bundesverwaltung ganz, ganz großen Stellenwert einzuräumen und vor allen Dingen auch, um die Krisenfähigkeit der Verwaltung zu verbessern. Wir sprechen sehr viel über Gesamtverteidigung, wir sprechen über die militärische Verteidigung, wir sprechen aber auch über die zivile Verteidigung. Und ganz entscheidend im Rahmen der zivilen Verteidigung ist ja auch die Aufrechterhaltung der Funktionsfähigkeit des Staates und seiner Regierungsfunktionen, aber genauso auch die Aufrechterhaltung der kritischen Infrastruktur im Sinne der Versorgung der Zivilbevölkerung. Also, es sprechen aus meiner Sicht sehr viele Gründe dafür, um auch aus dem Blickpunkt der zivilen Verteidigung dem Bundes-CISO eine starke Rolle am Tische des Nationalen Sicherheitsrates zu geben. Danke für die Frage.

Amt. Vors. **Josef Oster** (CDU/CSU): Vielen Dank. Und die Linke hat auch Fragenbedarf, sehe ich. Frau Vogtschmidt.

Abg. **Donata Vogtschmidt** (Die Linke): Vielen Dank. Ich hatte noch eine Frage an Herrn Dr. Herpig, und zwar: Wäre NIS-2 denn nicht auch ein Anlass dafür, das BSI endlich von den Aufgaben der Unterstützung von Sicherheitsbehörden zur Wahrung ihrer Aufgaben zu befreien? Ist es nicht sinnvoll, das zu 100 Prozent einfach an die Zentrale Stelle für Informationstechnik im Sicherheitsbereich (ZITiS) auszulagern, damit sich das BSI dann auch zu 100 Prozent auf die IT-Sicherheit konzentrieren kann, bezogen nicht nur auf die strukturelle Stellung des BSI, sondern einfach auch konkret auf die Aufgabenbeschreibung des BSI im Gesetzentwurf?

Amt. Vors. **Josef Oster** (CDU/CSU): Danke. Eine Frage an Herrn Dr. Herpig. Bitte schön.

SV **Dr. Sven Herpig** (interface): Das ist in der Tat so. Man könnte natürlich die NIS-2-Umsetzung dazu nutzen, dass man die entsprechenden Absätze ändert. Das ist allerdings nicht so ganz einfach wegen den Meldepflichten. Wenn das BSI zum Beispiel Informationen über eine Schwachstelle an das Bundesamt für Verfassungsschutz weitergibt, dann kann es diese Schwachstelleninformationen bekommen, weil es vielleicht diese Software einsetzt, die es eigentlich dazu nutzen soll, seine eigene IT abzusichern. Ob es damit dann andere Sachen macht, ist nicht ganz ersichtlich. Das heißt auch hier, ja, kann man machen, dann sind wir aber wieder bei einem umfassenden Ansatz des Schwachstellenmanagements, wie man es regeln würde. Das ist dann vielleicht nicht die ganz große Goldrandregelung, aber es ist auch nicht die ganz kleine Regelung, wo man einfach nur Sicherheitsforschende schützt und alles, was in diesem Gesetz zu Schwachstellen steht, nur dazu verwendet, um IT-Sicherheit herzustellen, sondern es wäre wieder eine erweiterte Version, die man noch einmal erarbeiten müsste, aber auch könnte, und dementsprechend ist es wieder zu vielen anderen Punkten zurückzuführen, die wir gerade diskutiert haben: Wie viel Zeit wollen wir noch einräumen, dieses Gesetz umzusetzen? Und es ist definitiv nicht etwas, was in der engen Auslegung einer NIS-2-Umsetzung geschehen müsste, aber definitiv etwas, was man machen könnte. Da kommt es eben darauf an, wie viel Zeit wir uns nehmen wollen. Wir haben hier schon verschiedene Perspektiven gehört, entweder schnell oder richtig umfassend. Das kann ich nicht beantworten, aber wenn man sich noch ein bisschen mehr Zeit nimmt, könnte man das definitiv entsprechend noch einbauen und umsetzen und das BSI und die Schwachstellenmeldungen ans BSI und im Sinne der IT-Sicherheit, zum Schutz der Systeme abkoppeln von entsprechenden Übermittlungsbefugnissen oder Übermittlungsmöglichkeiten des BSI an Schwachstellen, an andere Behörden, die das eventuell nicht dazu nutzen, IT-Sicherheit herzustellen, sondern IT-Sicherheit zu unterminieren. Das ist in der Tat so.

Amt. Vors. **Josef Oster** (CDU/CSU): Danke, Herr Dr. Herpig. Damit sind wir auch mit der dritten Fragerunde am Ende. Ich sehe jetzt keine weitere zwingende Wortmeldung mehr, sodass wir dann unsere Anhörung hier beenden können. Ich darf mich bei allen, die heute hier teilgenommen haben, sehr herzlich bedanken. Es ist eine zweifellos hochaktuelle und spannende Thematik, mit der wir uns heute hier auseinandergesetzt haben. Ich darf mich bei den Sachverständigen für Ihre Bereitschaft herzlich bedanken, dass Sie uns heute hier Rede und Antwort gestanden haben mit Ihrer Expertise. Die ist heute gebraucht worden und wird auch in Zukunft weiterhin benötigt werden. Deshalb vielen Dank für heute. Den Kolleginnen und Kollegen vielen Dank für die Teilnahme an der Anhörung. Auch der Parlamentarischen Staatssekretärin ein herzliches Dankeschön. Ich schließe damit die Sitzung und wünsche Ihnen noch einen schönen Tag.

Schluss der Sitzung: 16.42 Uhr

Josef Oster, MdB
Amtierender Vorsitzender