bitkom

Auf einen Blick

# Stellungnahme zum Eckpunktepapier der Cyber-Sicherheitsstrategie 2021

## Bitkom-Bewertung

Die neue CSS 2021 muss glaubhaft die Ambition erkennen lassen die bisherigen Fehlkalibrierungen im Bereich der Cybersicherheit zu überwinden und die vielen verschiedenen losen Enden langfristig, nachhaltig und sicherheitssteigernd zusammenzubringen. Das vorliegende Eckpunktepapier lässt eine positive Gesamttendenz erkennen und ist aus Sicht des Bitkom begrüßens- und unterstützenswert. Allerdings gilt es die folgenden Punkte zu berücksichtigen:

- **Leitlinie 1 – Digitale Souveränität**
  Cybersicherheit muss als Rückgrat für die erfolgreiche digitale Transformation und Garant Digitaler Souveränität wahrgenommen werden. Um den dafür notwendigen Awareness-Schub zu befördern, darf Cybersicherheit nicht bloß als Add-on der Produktentwicklung verstanden werden sondern ist selbst als digitale Schlüsseltechnologie zu begreifen. Bitkom erachtet die Aufnahme dieses Standpunkts in die CSS 2021 als notwendig und zielführend.
- **Leitlinie 2 – Sichere Gestaltung der Digitalisierung**
  Es bedarf weniger der zusätzlichen strategischen Formalisierung – die Zielsetzung wird uneingeschränkt geteilt. Bottleneck ist die praktische Umsetzung. Es bedarf mehr Tatkraft und Pragmatismus statt strategischer Perfektion.
- **Leitlinie 3 – Effektivität und Messbarkeit**
  Bitkom begrüßt ausdrücklich, dass die von uns befürwortete und geforderte Erfolgsmessung Einzug in die CSS 2021 erhält. Allerdings reichen die besten und geeignetsten Indikatoren nicht aus, um einen positiven Wandel einzuläuten. Es kommt darauf an, die Resultate fachkundig zu interpretieren und die offengelegten Handlungsbedarfe konsequent anzugehen – auch die unbequemen.

- **Handlungsfeld 1 – Sicheres und selbstbestimmtes Handeln in einer digitalisierten Umgebung**
  Mit der CSS 2021 muss ein Narrativwechsel eingeleitet werden: weg von einem unsicherheits- und notgetrieben Cybersicherheitsverständnis hin zur positiv konnotierten und incentivierenden Cybersicherheitswahrnehmung.
- **Handlungsfeld 2 – Gemeinsamer Auftrag von Staat und Wirtschaft**
  Bitkom bekennt sich klar zum gemeinsamen Auftrag von Staat und Wirtschaft die Cybersicherheit Deutschlands zu erhöhen. Die der Zusammenarbeit zwischen Staat und Wirtschaft innewohnenden Gestaltungskraft kann nicht überschätzt werden. Allerdings sind die beschworene Zusammenarbeit sowie der vertrauensvolle Austausch dann aber auch in der Praxis mit Leben zu füllen.
- **Handlungsfeld 3 – Leistungsfähige und nachhaltige gesamtstaatliche Cyber-Sicherheitsarchitektur**
  Aktuell dominiert der ‘Aus- und Aufbau‘ sowie die ‘Erweiterung und Vertiefung‘ das Handlungsfeld. Der Blind Spot ist die Bereitschaft, die bisherige Architektur zu entschlacken, zu straffen und effizienter zu organisieren. Die neue Strategie darf nicht den Weg des geringsten Widerstands gehen.
- **Handlungsfeld 4 – Aktive Positionierung D. in der europäischen und internationalen Cyber-Sicherheitspolitik**
  Bitkom betont nachdrücklich die Relevanz eines europäisch einheitlichen strategischen Vorgehens. Ein Divergieren künftiger nationalstaatlicher Cybersicherheitsstrategien muss um jeden Preis verhindert werden. Erfolgskritischer Faktor der CSS 2021 ist die 100 prozentige Übereinstimmung mit den (neuen) Anforderungen der NIS2-Richtlinie.

# Stellungnahme zum Eckpunktepapier der Cyber-Sicherheitsstrategie 2021

14. April 2021


**Vorbemerkungen**

Bitkom begrüßt ausdrücklich, dass sich die Bundesregierung intensiv mit der Fortschreibung der Nationalen Cyber-Sicherheitsstrategie (CSS 2021) auseinandersetzt und die Wirtschaft bei der Entwicklung der strategischen Ziele und operativen Maßnahmen involviert. Auf diese Weise lassen sich sinnvolle Anforderungen auf den Weg bringen, deren Machbarkeit dann auch gewährleistet ist und von der Wirtschaft unterstützt wird. Die unter Beteiligung von Vertretern aus Wirtschaft, Wissenschaft und Wirtschaft durchgeführten Evaluations-Workshops zur CSS 2016 waren bereits ein wichtiger Schritt, um die Grundausrichtung des künftigen strategischen Rahmens in geeigneter Art und Weise abzustecken.

Mit der CSS 2021 werden die „*Digitale Souveränität*“, die „*Sichere Gestaltung der Digitalisierung*“ sowie die „*Effektivität und Messbarkeit*“ als übergeordnete inhaltliche Leitlinien eingezogen. Darüber hinaus unterscheidet die CSS 2021 zwischen strategischen Zielen und operativen Maßnahmen. Beide sollen in der aktuellen Fortschreibung erarbeitet werden. Strategische Ziele werden jeweils einem Handlungsfeld zugeordnet und adressieren die zentralen Herausforderungen des Handlungsfeldes. Anknüpfend an die CSS 2016 soll sich die CSS 2021 (weiterhin) in die folgenden vier Handlungsfelder auffächern:

1. *Sicheres und selbstbestimmtes Handeln in einer digitalisierten Umgebung;*
2. *Gemeinsamer Auftrag von Staat und Wirtschaft;*
3. *Leistungsfähige und nachhaltige gesamtstaatliche Cyber-Sicherheitsarchitektur;*
4. *Aktive Positionierung Deutschlands in der europäischen und internationalen Cyber-Sicherheitspolitik.*

Zur Begegnung und Bewältigung neuer strategischen Herausforderungen wird dieses bestehende Grundgerüst um neue strategische Ziele aktualisiert und ergänzt, die SMART (spezifisch, messbar, aktiv beeinflussbar, realistisch und terminiert) sein sollen. Neben strategischen Zielen beschreiben die operativen Maßnahmen Aktivitäten, mit denen die strategischen Ziele erreicht werden sollen. Sie müssen geeignet sein, das jeweilige strategische Ziel in der Laufzeit der CSS 2021 vollständig zu erreichen.

Bitkom
Bundesverband
Informationswirtschaft,
Telekommunikation
und Neue Medien e.V.

**Sebastian Artz**
**Referent Informationssicherheit & Sicherheitspolitik**
s.artz@bitkom.org

Albrechtstraße 10
10117 Berlin

Präsident
Achim Berg

Hauptgeschäftsführer
Dr. Bernhard Rohleder

Bitkom erachtet das gewählte Vorgehen als zielführend und unterstützenswert. An der Beibehaltung der vier Handlungsfelder ist nichts auszusetzen. Zudem beinhaltet das vorliegende Eckpunktepapier eine Vielzahl von richtigen Punkten, deren strategische Berücksichtigung zwingend notwendig ist. Wichtig ist auch, dass diese Eckpunkte als gemeinsame, von allen Ressorts der Bundesregierung mitgetragene Grundlage für die Erstellung der CSS 21 dienen soll. Deutschland hat auf dem Gebiet der Digitalisierung stark aufzuholen. Die Verringerung des „digitalen Hinterherhinkens" kann nur gelingen, wenn mit der Digitalisierung zeitgleich Maßnahmen zur Erhöhung der Cybersicherheit wirksam auf den Weg gebracht und umgesetzt werden. Nur so ist eine sichere Nutzung digitaler Dienste möglich und die Bereitschaft der Inanspruchnahme solcher Dienste durch Staat, Wirtschaft und Bevölkerung zu erreichen bzw. zu erhöhen. Dabei darf die CSS 2021 nicht wieder ein Sammelsurium von Einzelmaßnahmen werden, sondern muss einem orchestrierenden Leitgedanken folgen. Die vorgesehene Flankierung der Handlungsfelder durch übergeordnete Leitlinien ist somit ausdrücklich zu begrüßen.

Trotz dieser positiven Gesamteinschätzung bleiben die mit der CSS 2021 verfolgten Ambitionen ein Stück weit hinter den Erwartungen zurück. Mehr operative Meilensteine würden nicht nur dem selbstgesteckten Ehrgeiz gut tun sondern auch ein wichtiges Signal für das Gesamtökosystem darstellen. Zudem stehen die Eckpunkte unter Haushaltsvorbehalt (bzgl. Ausgabemitteln und Personal). Mit Blick auf die nächste Legislaturperiode stellt sich die Frage der Durch- und Umsetzbarkeit der Eckpunkte.

Der Erfolg der neuen CSS wird vor allem auch von der Fähigkeit abhängen, Zielkonflikte zwischen den für sich alleine stehenden sinnvollen Einzelaspekten im Zeitverlauf zu identifizieren und aufzulösen. Der Grad der dafür notwendigen inhärenten Grunddynamik der CSS 2021 wird einen wesentlichen Erfolgsfaktor darstellen.

Das Eckpunktepapier lässt aktuell auch noch keine klare Richtschnur erkennen, wie Wachstumschancen der mittelstandsgeprägten deutschen IT-Sicherheitsindustrie verbessert werden sollen. Im weiteren Ausgestaltungsprozess der CSS 2021 wird es darauf ankommen, die bereits aufgelisteten Pläne und Fähigkeitsanalysen mit den nationalen Beschaffungsstrukturen in Einklang zu bringen und die bestmögliche Auswahl aus dem international verfügbaren Leistungsportfolio zu treffen.

Daneben haben wir in unserer Stellungnahme zum IT-Sicherheitsgesetz 2.0 bereits deutlich gemacht, dass es in Anbetracht des wechselseitigen Zusammenspiels einer Vielzahl von Regelungsgegenstände dringend geboten ist, die Konsolidierung der Gesetzestexte eng und widerspruchsfrei zu fassen und Redundanzen auszuschließen. Komplexität ist und bleibt der größte Feind von Sicherheit. Das gilt ebenso sehr auf regulatorischer Ebene wie für das Zusammenwirken der verschiedenen Institutionen auf

Ebene der Länder, des Bundes sowie der EU. Auch wenn es sich bei diesen regulatorischen und institutionellen Aspekten nur um zwei Facetten des großen Ganzen handelt, darf es in der CSS 2021 keine unadressierten „blind spots“ geben. Alles, was die Cybersicherheit in der Breite betrifft und beeinflusst, muss strategisch mitgedacht und im Zuge der Überarbeitung der CSS 2021 konsequent auf den Prüfstand gestellt und ergebnisneutral bewertet werden.

## Inhalt

Seite

## 1 Leitlinie „Digitale Souveränität“

Die Festlegung auf Digitale Souveränität als zentrale Leitlinie der CSS 2021 ist aus Sicht des Bitkom ausdrücklich zu begrüßen. Mit einer Erhöhung der digitalen Souveränität Deutschlands und Europas werden Beiträge in allen Handlungsfeldern ermöglicht oder bewerkstelligt. Insoweit kommt diesem Punkt eine herausgehobene Bedeutung zu, die sich in der CSS 2021 widerspiegeln muss. Bitkom begrüßt, dass in der CSS 2021 das von IT-Rat und IT-Planungsrat abgestimmte Verständnis „Digitaler Souveränität“ zugrunde gelegt wird. Damit ist ebenso klar, dass nicht nur einzelne Maßnahmen, sondern ein Kultur- und Wahrnehmungswandel hinsichtlich IT-Sicherheit in Gesellschaft, Wirtschaft und öffentlicher Verwaltung gleichermaßen notwendig sind. Entscheidend ist dabei eine stärkere Herausarbeitung eines risikoorientierten Ansatzes in der CSS 2021. Aktuell stellt sich die Frage, welches Handlungsfeld sich mit der ‚Risikobewertung‘ für die verantwortungsvolle und sichere Einführung verfügbarer Technologie beschäftigt (vorwärts gerichteter Ansatz, keine Risikobewertung im Sinne von ‚warum kann ich etwas nicht nutzen‘)? Zudem bleibt das Verhältnis von Cybersicherheit und Digitaler Souveränität zueinander unklar. Die CSS 2021 sollte Klarheit bzgl. der begrifflichen Wechselbeziehung schaffen.

Das Narrativ darf sich dabei aber nicht aus protektionistischen Überlegungen und Autarkiebestrebungen speisen sondern muss von der Ambition geprägt sein, transnationale Arbeitsteilung souverän zu nutzen und sämtliche Sicherheitstechnologien technisch vollumfänglich zu verstehen, wirtschaftlich anzuwenden und forschungsgetrieben weiterzuentwickeln. Nur so lassen sich bestehende Gestaltungsspielräume erhalten und neue technologische Freiheitsgrade hinzugewinnen. Zudem sollte stets eine europäische Ausrichtung das Ziel sein.

Für sicherheitskritische Komponenten und Lösungen im hoheitlichen Umfeld sind eine langfristige Verfügbarkeit von Support, Service und technischer Weiterentwicklung unabdingbar. Die Anbieter müssen Lösungen bereitstellen und entsprechend dem technologischen Wandel derart weiterentwickeln können, dass eine umfassende IT-Sicherheit unabhängig vom Plattformanbieter oder Netzwerkausrüster gewährleistet wird.

Sowohl national als auch auf EU-Ebene wird viel in Cybersecurity-Forschung investiert. Dies allein ist jedoch nicht hinreichend, um dem Ziel digitaler Souveränität näher zu kommen: Hierfür braucht es neben einheitlichen rechtlichen Rahmenbedingungen in der EU auch einen berechenbaren Nachfragemarkt. Dieser ist Grundvoraussetzung dafür, dass die staatlichen Forschungsausgaben tatsächlich zu zielgerichteten Investitionen der Industrie und damit einer Stärkung der digitalen Souveränität Deutschlands und Europas führen.

## 2 Leitlinie „Sichere Gestaltung der Digitalisierung“

Bitkom unterstützt vollumfänglich das Ziel einer sicheren Digitalisierung und sieht ebenfalls die Notwendigkeit, der querschnittlichen Logik der Zielsetzung mit einer übergeordneten Leitlinie Rechnung zu tragen.

Konkret wird argumentiert, dass die „[...] *digitale Transformation von Staat (z.B. E-Governmentgesetz, Onlinezugangsgesetz, IT-Konsolidierung, Mobiles Arbeiten etc.), Wirtschaft (z.B. Sicherheitsanforderungen an 5G-Netze) und Gesellschaft (z.B. eID, Homeschooling etc.) wesentlich an Dynamik gewonnen. Deren sichere Ausgestaltung ist Voraussetzung dafür, dass Digitalisierung souverän und zum Vorteil der Menschen in Deutschland gelingt.*“ Bitkom teilt die Einschätzung und erachtet die Spezifizierung entsprechender strategischer Ziele grundsätzlich für sinnvoll. Allerdings stellt sich die Frage, wo dieser Ansatz in der aktuellen Pandemiesituation zu sinnvollen Lösungen beigetragen hat. Hier könnte SMART ansetzen und fragen: welchen Beitrag haben die aktuellen Gesetzgebungsvorhaben (wie aufgeführt) zur Bewältigung der bundesweiten Krisensituation beigetragen? Auch muss an dieser Stelle darauf hingewiesen werden, dass es aktuell weniger an der strategischen Formulierung einer solchen Leitlinie sondern vielmehr an deren praktischen Umsetzung mangelt. Der Entstehungsprozess des IT-Sicherheitsgesetzes 2.0 sei an dieser Stelle exemplarisch angeführt. Die Dynamik, die im Eckpunktepapier der digitalen Transformation zugeschrieben wird, muss in gleicher Manier im Gesetzgebungsprozess Berücksichtigung finden. Einerseits dürfen die Legislativvorhaben nicht nur für sich alleine stehen sondern müssen sich nahtlos in die nationale und europäische Gesamtarchitektur einfügen. Andererseits sind die Legislativvorhaben derart auszugestalten, dass die dynamischen technologischen Weiterentwicklungen der Praxis bereits im Erarbeitungsprozess eingepreist werden. Ziel muss es sein, langfristig tragfähige Rahmenwerke zu schaffen. Dazu sollten die EU-Gesetzgeber verstärkt mit der Cybersecurity-Industrie zusammenarbeiten. Der gegenwärtigen Fragmentierung der Cyber-Sicherheitsvorschriften in den EU-Mitgliedsstaaten wäre u.a. auch mit einer umfänglichen gemeinsamen Anerkennung von Zulassungen entgegenzuwirken.

Hervorgehoben sei zudem, dass die sichere Gestaltung der Digitalisierung Transparenz erfordert: in den Lieferketten, den Standards und Architekturen, der Software und auch der Hardware bis in die sichere vertrauenswürdige Mikroelektronik hinein. Hier sind globale Konstellationen entstanden, die es strategisch stufenweise zu adressieren gilt.

## 3 Leitlinie „Effektivität und Messbarkeit der CSS 2021“

Eine gemeinsame, nicht repräsentative Umfrage von DIHK, BDI und Bitkom im September 2020 hat verdeutlicht, dass trotz des umfangreichen Aufbaus von Stellen in BSI und BMI sowie der zahlreichen initiierten Maßnahmen (u.a. Nationaler Pakt für Cybersicherheit, Initiative IT-Sicherheit in der Wirtschaft) vielfach Unternehmen die Ziele der CSS 2016 als nicht umgesetzt erachten. Dies liegt gewiss darin begründet, dass beim Verfassen der CSS 2016 auf die Nennung konkreter Meilensteine sowie eines klaren Zeitplans verzichtet wurde.

Vor dem Hintergrund begrüßt Bitkom ausdrücklich, dass die von uns befürwortete und geforderte Erfolgsmessung Einzug in die CSS 2021 erhält. Wenngleich auch nicht jede Bemühung bei der Erhöhung der Cyber-Sicherheit messbar sein wird, so ist die Einführung der Leitlinie „Effektivität und Messbarkeit“ eine wichtige Komponente um die Digitalisierung des Landes und die Erhöhung der Sicherheit schneller vorantreiben zu können. Da wo gemessen werden kann, bspw. wie viele Schüler sich einen Rechner in Deutschland teilen müssen, sollte ein Controlling möglich und ein erforderliches und zeitnahes Nachsteuern gewährleistet sein.

Einer der angeführten Eckpunkte lautet: „*Die Umsetzung der einzelnen Maßnahmen zur Zielerreichung der CSS 2021 soll dezentral im Rahmen des Ressortprinzips erfolgen. Zur Steuerung und Überwachung der Umsetzung der Maßnahmen werden durch die Strategie keine Vorgaben gemacht*.“ Dies ist wenig ambitioniert. Das dezentrale Schultern der Maßnahmen durch die verschiedenen Ressorts ist sinnvoll. Es erschließt sich aber nicht, weshalb keine konkreten Vorgaben bei der Umsetzung für die einzelnen Ressorts oder zumindest von diesen selbst gemacht werden, die dann ihrerseits beim Controlling genutzt werden können. Zudem sollte ein positiv konnotierter und incentivierender Wettbewerb zwischen den Ressorts aktiv befördert werden. Denkbar wäre die Schaffung von Sichtbarkeit und Präsentationsmöglichkeiten für besonders erfolgreich operierende Ressorts im Rahmen der Sitzungen des Nationalen Cyber-Sicherheitsrates.

Daneben wird in einem weiteren Eckpunkt skizziert, dass: „*[u]m das Controlling möglichst effizient zu gestalten, geeignete und bereits bestehende Erhebungen, Prüfungen und Kennzahlen zum Stand der Cyber-Sicherheit in Bund und Ländern in die Indikatoren der CSS 2021 einfließen und gegebenenfalls ergänzt und vereinheitlicht werden sollen*.“ Bitkom fordert die Definition geeigneter Kennzahlen, die den Einfluss der CSS2021 auf die wirtschaftlichen KPIs widerspiegeln und die im Konsens zwischen Verwaltung, Wirtschaft und Gesellschaft definiert werden. Anstelle weiterer technischen ‚Cyber‘-Metriken, wie die Anzahl betroffener Krankenhäuser, bedarf es verstärkt der Abbildung von Chancen der CSS2021. Ein potenzieller Ansatzpunkt wäre bspw. die Frage: wie schnell

Technologielösungen (bspw. Videokonferenzlösung oder E-Mail-Systeme) als Lösungspakete bewertet und für den Einsatz grundsätzlich frei gegeben werden können (Stichwort Pandemiebewältigung)? Es ist stärker in Richtung pauschaler Risikobewertung zu denken (im Kontext des jeweiligen Anwendungsfalls), statt tausendfacher, langwieriger Einzelprüfungen durch Betroffene (die häufig nicht über die Notwendigen Fachkenntnisse verfügen und dringend Hilfe suchen).

Der Fokus muss ganz klar auf „geeigneten" Kennzahlen liegen, nicht auf den „bereits bestehenden". Letztere können zweifelsohne weiterhin notwendig sein. Allerdings darf eine neue Strategie nicht den Weg des geringsten Widerstands gehen. Aus der Verwendung des Wortes „gegebenenfalls" spricht ein nicht ausreichender Änderungswille. Alle bestehende Maßnahmen und Kennzahlen müssen konsequent auf den Prüfstand gestellt und ergebnisneutral bewertet werden. Allerdings darf nicht vergessen werden, dass die besten und geeignetsten Indikatoren nicht ausreichen, um einen positiven Wandel einzuläuten. Es kommt darauf an, die Resultate fachkundig zu interpretieren und die sich daraus ergebenen Handlungsempfehlungen konsequent umzusetzen – auch die unbequemen.

Der letztgenannte Eckpunkt besagt, dass: „*betroffene Akteure außerhalb des Staates (z.B. Hersteller, Dienstleister, Hochschulen) sollen in den Überprüfungsprozess einbezogen werden. Hierfür sollen Kommunikationsprozesse für diese Akteure implementiert werden*." Bitkom begrüßt die vorgesehene Einbeziehung der relevanten Akteure in den Überprüfungsprozess. Gerne stehen wir in den kommenden Jahren unterstützend zur Verfügung. Allerdings erschließt es sich nicht, weshalb lediglich eine „Einbeziehung" der genannten Akteure stattfinden soll und dafür extra Kommunikationsprozesse zu implementieren sind. Zielführender und wünschenswert wäre eine „gemeinsame Überprüfung mit der Wirtschaft". Bestehende Kommunikationsprozesse ließen sich dabei schnell und ressourcenschonend nutzen.

# 4 Handlungsfelder

## 4.1 Handlungsfeld 1 – Sicheres und selbstbestimmtes Handeln in einer digitalisierten Umgebung

Cybersicherheit muss als Rückgrat für die erfolgreiche digitale Transformation wahrgenommen werden. Um den dafür notwendigen Awareness-Schub zu befördern, darf Cybersicherheit nicht bloß als Add-on der (End-)Produktentwicklung verstanden werden sondern muss selbst als digitale Schlüsseltechnologie begriffen werden. Bitkom erachtet die Aufnahme dieses Standpunkts in die CSS 2021 als notwendig und zielführend.

Die gelisteten Eckpunkte sehen u.a. vor, dass digitale Produkte und Dienstleistungen, die im EU-Binnenmarkt angeboten werden, Aspekte der Cyber- und Informationssicherheit als Qualitätsmerkmal beinhalten. Bitkom empfiehlt, das Qualitätsmerkmal „Made in Europe" einer alleinigen deutschen Fokussierung vorzuziehen. Außerdem soll das Engagement für die Einführung eines europaweit gültigen Kennzeichens mit verbindlichem Charakter in der Cybersicherheitsstrategie 2021 festgeschrieben werden. Für die Umsetzung beider Aspekte gibt es auf europäischer Ebene bereits ein etabliertes System, dass sich mit Blick auf Produktsicherheit, Nachvollziehbarkeit und Verbrauchervertrauen bewährt hat: Das New Legislative Framework (NLF; neuer Rechtsrahmen). Der Gesetzgeber beschränkt sich dabei auf das Festlegen von Schutzzielen und verweist zu deren technischer Ausgestaltung auf harmonisierte Europäische Normen. Im analogen Bereich ist dieses Prinzip die Basis für europaweit harmonisierte Anforderungen und den funktionierenden Binnenmarkt. Jetzt gilt es, diesen Ansatz auf den digitalen Binnenmarkt zu übertragen. Dafür braucht es eine geeignete europäisch horizontale Cybersicherheitsregulierung. Wie diese aus Sicht des Bitkom ausgestaltet werden sollte, kann hier im Detail nachgelesen werden.

Bitkom empfiehlt zudem die Aufnahme und Ergänzung der folgenden Eckpunkte:

+ Neuer Eckpunkt: *EU-Gesetzgeber sollten zusammenarbeiten, um eine Fragmentierung der Cyber-Sicherheitsvorschriften in verschiedenen Märkten zu vermeiden. Ein europaweiter, harmonisierter Cybersicherheits-Zertifizierungsrahmen ist erforderlich. Bestehende Cyber-Zertifizierungen sollten faire Bedingungen für die Erneuerung und konsequente gegenseitige Anerkennung erhalten; zwischen neuen und bestehenden Zertifizierungssystemen sollte gegenseitige Anerkennung und Abstimmung hergestellt werden.*
+ Neuer Eckpunkt: *E-labelling sollte als Alternative zu physischen Etiketten vorangetrieben werden, um die Transparenz für Verbraucher durch stets aktualisierte Informationen zu erhöhen.*
+ Eckpunkt-Ergänzung: *Insbesondere soll die Sicherheit von Schlüssel- und Zukunftstechnologien i. S. e. "Security by Design"-Ansatzes von vornherein mitgedacht und gestärkt werden. Das gilt nicht nur für Hersteller von Softwareprodukten oder digitalen Diensten, sondern auch für Endgeräte. Die Zahl von Endgeräten wird sich mit der Etablierung neuer Anwendungen (IoT) vervielfachen. Zudem sollte Security by Design auch für E-Government Lösungen und Verwaltungshandeln gelten, gemäß eines risikobasierten Ansatzes. Es gilt, die Information(en) zu schützen. Dies erfordert das dafür notwendige Prozessdenken.*

Darüber hinaus ist es wichtig, klare Forschungs- und Förderschwerpunkte für den Erhalt bzw. den Auf- und Ausbau der industriellen Kompetenzen und Kapazitäten zu definieren und zu fördern: Mikro- und Nanoelektronik, Rechenzentren und Cloud-Infrastrukturen, Hochleistungsrechner und Quantencomputer sowie Kommunikationssysteme und Netze stellen die Infrastruktur- und Hardwaregrundlagen der Digitalisierung dar. Kompetenzen und Kapazitäten in Forschung, Entwicklung und Herstellung dieser Komponenten sind Garanten für Wachstum und Souveränität. Bitkom begrüßt daher ausdrücklich das Vorhaben, quantentechnologische Verfahren, Mikro- und Nanoelektronik sowie die Fortentwicklung von Netzwerkkomponenten im Sinne der Stärkung der Digitalen Souveränität des Standorts zu fördern. Dabei muss jedoch stets ein technologieunabhängiger Ansatz forciert werden. Denn nur so kann es uns gelingen, neue Entwicklungen frühzeitig zu erfassen und faire bzw. wettbewerbsorientierte Bedingungen für alle Unternehmen gleichermaßen zu schaffen. Im Sinne einer klugen Standortpolitik darf es gleichwohl nicht dazu kommen, einzig auf in Deutschland vorhandene Fähigkeiten zu fokussieren, ohne die Attraktivität des Standorts insgesamt zu fördern. Ein Beispiel hierfür ist der bereits heute massive Mangel an Fachkräften und Talenten, dem nur durch Internationalisierung begegnet werden kann. Zur Stärkung der Attraktivität des Standorts, von Partnerschaften und Ökosystemen gehört weiterhin, dass durch Steuergelder geförderte Forschungsergebnisse nicht in Drittstaaten zur Marktreife geführt werden. Ein dritter Aspekt der Standortsicherung ist, die Anwendung von anerkannten Schlüsseltechnologien im nationalen Sicherheitsinteresse gemäß den vergaberechtlichen Vorgaben zu nutzen. Der vierte Aspekt adressiert die Stärkung der Fähigkeit, potenzielle Sprunginnovationen frühzeitig zu erkennen, sie mit geeigneten Förderinstrumenten zur Marktreife zu bringen und am Weltmarkt zu etablieren. Dies weist zurück auf die erwähnten Partnerschaften und Ökosysteme. Im Digitalzeitalter ist Industriepolitik gleichbedeutend mit Innovations- und Digitalpolitik. Existierende Instrumente, wie etwa die wichtigen Vorhaben von gemeinsamem europäischem Interesse (IPCEI), müssen verstärkt für digitale Technologien erschlossen werden. Durch die kurzen Innovationszyklen gilt es darüber hinaus diese Instrumente sachgerecht weiterzuentwickeln und inhaltlich den besonderen Bedingungen der digitalen Wirtschaft anzupassen. Es bedarf einer klugen, wettbewerbsorientierten Industriepolitik, die transnationale Arbeitsteilung souverän nutzt und von der Forschung über die Entwicklung bis hin zur Beschaffung leistungsorientierte Technologien fördert. Parallel dazu gilt es natürlich weiterhin die technologisch unverzichtbare Grundlagenforschung aufrechtzuerhaltenden.

Bitkom erachtet eine konsequente Förderung des Einsatzes für sichere Verschlüsselung am Standort Deutschland für richtig. Dies beinhaltet gleichzeitig eine Klärung der „deutschen Krypto-Strategie“, wie sie im Eckpunkt „*Die Ziele der deutschen Krypto-Strategie sollen weiterhin konsequent verfolgt werden, um den umfassenden Schutz der*

*Bürgerinnen und Bürgern sowie unserer Wirtschaft und Institutionen (Gruppen und Gemeinschaften, z.B. Vereine und Organisationen) vor Cyber-Gefahren zu gewährleisten*." erwähnt wird. Was ist die ‚deutsche Krypto-Strategie'? Wie passt diese in CSS 2021? Welchen realen Impact hat die CSS2021 in Kombination mit der ‚dt. Kryptostrategie' für „Vereine" und „Organisationen"? Es gilt ihre Ziele und Mittel, ihre technologischen Grundlagen bzw. Voraussetzungen, ihre Angemessenheit sowie damit ihre Reichweite zu definieren.

## 4.2 Handlungsfeld 2 – Gemeinsamer Auftrag von Staat und Wirtschaft

Das Handlungsfeld wird mit dem folgenden Satz eingeleitet: „*Ein enger Austausch zwischen Staat und Wirtschaft ist unabdingbar, um Cyber-Sicherheit in Deutschland dauerhaft auf einem hohen Niveau gewährleisten zu können.*" Bitkom stimmt dieser Aussage – deren innewohnende Gestaltungskraft nicht überschätzt werden kann – zu 100 % zu. Allerdings sind die beschworene Zusammenarbeit sowie der vertrauensvolle Austausch dann aber auch in der Praxis mit Leben zu füllen. Bitkom bekennt sich klar zum gemeinsamen Auftrag von Staat und Wirtschaft die Cybersicherheit Deutschlands zu erhöhen.

Bitkom begrüßt, dass die Stärkung der Arbeit internationaler Standardisierungs-organisationen und -gremien in der CSS 2021 aktiv adressiert und die Notwendigkeit einheitlicher Anforderungen hervorgehoben werden soll. Im Bereich IT-Sicherheit hält Deutschland über DIN und DKE mit der Führung zentraler europäischer (CEN/CENELEC JTC 13 „Cybersecurity and Data Protection") und internationaler (ISO/IEC JTC1/SC 27 „Information Security, Cybersecurity and Privacy Protection"; IEC/TC 65/WG 10 "Security for industrial process measurement and control - Network and system security") Arbeitsgremien die Marktführerschaft in der IT-Sicherheits-Standardisierung. In diesen Gremien werden grundlegende Normen zur IT-Sicherheit gepflegt, beispielsweise die DIN EN ISO/IEC 27000-Normenreihe für „Informationssicherheit-Managementsysteme", die ISO/IEC 15408 „Evaluationskriterien für IT-Sicherheit" oder die Normenreihe IEC 62443 „Industrielle Kommunikationsnetze - IT-Sicherheit für Netze und Systeme". Diese internationalen Normen werden von deutschen Unternehmen erfolgreich angewendet. Eine starke deutsche Position in der IT-Sicherheitsnormung stärkt darüber hinaus die deutsche IT-Wirtschaft. Deshalb sollte Deutschland politische Prioritäten strategisch in der internationalen Normung unterstützen, z. B. durch finanzielle Förderung der deutschen Projektleitung und Beteiligung in den identifizierten Bereichen.

Um Normen und Standards im Bereich Cyber-Sicherheit europaweit einheitlich zu definieren kann die Europäische Kommission bereits jetzt nach Artikel 10 der Verordnung

(EU) Nr. 1025/2012 Normungsaufträge an die Europäischen Normungsorganisationen CEN, CENELEC und ETSI erteilen. Von diesem Instrument sollte vermehrt Gebrauch gemacht werden.

Um den Spagat zwischen Usability und Security zu bewerkstelligen, ist ein engerer Schulterschluss zwischen Staat und IT- und Cybersicherheits-Industrie bereits im Vorfeld der Beschaffung notwendig.

Nachvollziehbar sind die Planungen, zum Schutz kritischer Infrastrukturen die Anforderungen an KRITIS-Betreiber auszubauen, Mindestanforderungen regelmäßig zu überprüfen und bei Bedarf anzupassen, damit der sich ändernde Stand der Technik durch die Betreiber erfüllt wird. Nur greift die einseitige Verpflichtung der KRITIS-Betreiber zu kurz. Alle Akteure der digitalen Wertschöpfungskette müssen Verantwortung übernehmen. Nur eine faire Lastenverteilung wird letztlich zu einer sicheren Digitalen Wirtschaft führen. Ein ganzheitlicher Ansatz, der auch die in kritischen Infrastrukturen eingesetzte Hard- und Software mitdenkt, würde zahlreiche potenzielle Sicherheitsprobleme bereits an der Wurzel angehen und vielfach direkt lösen.

Wir begrüßen die Absicht, die Beiträge von Unternehmen zur Detektion und Aufklärung von Bedrohungen zu erhöhen. Zielführend im Sinne eines ganzheitlichen Konzepts wird dieser Ansatz allerdings nur durch den gegenseitigen vertrauensvollen Austausch von Informationen zu Sicherheitslücken – auch von Seiten der Behörden in Richtung der Unternehmen. Solange den Sicherheitsbehörden Schwachstellen bekannt sind, welche von den Unternehmen – insbesondere den Betreibern kritischer Infrastruktur – mangels Kenntnis aber nicht geschlossen werden können, existieren potenzielle Angriffsziele und damit nicht zu unterschätzende Risiken. Der geforderte Wirschaftsschutz bleibt unvollkommen.

## 4.3 Handlungsfeld 3 – Leistungsfähige und nachhaltige gesamtstaatliche Cyber-Sicherheitsarchitektur

Handlungsfeld 3 macht es sich zur Aufgabe, eine zeitgemäße Cyber-Sicherheitsarchitektur zu forcieren: *„die die verschiedenen Akteure auf Bundesebene wirksam verzahnt und daneben Länder, Kommunen und Wirtschaft im Blick behält“*. Anstatt die Wirtschaft lediglich „im Blick zu behalten“ kommt es aber vor allem auf die aktive Einbindung und den Dialog mit der Wirtschaft an. Wie in der Vergangenheit steht Bitkom hierfür jederzeit gerne zur Verfügung und signalisiert auch in Handlungsfeld 3 konstruktive Gesprächsbereitschaft.

Neben den vielen wichtigen und unterstützenswerten Eckpunkten in Handlungsfeld 3 möchte Bitkom einen „blind spot“ deutlich hervorheben. Zunächst seien die folgenden Eckpunkt-Fragmente angeführt:

- *Die Cyber-Sicherheitsarchitektur des Bundes wird strukturell und prozessual einer Bewertung durch die Bundesregierung unterzogen.*
- *Um die effektive Zusammenarbeit zwischen Bund und Ländern **weiter zu vertiefen**, wird angestrebt, das BSI in seinem bestehenden Aufgabenbereich zu einer Zentralstelle im Bund-Länder-Verhältnis **auszubauen.***
- *Der verbindliche Austausch von Informationen innerhalb der Cyber-Sicherheitsarchitektur, insbesondere zwischen Bund und Ländern, sollte weiter intensiviert und **ergänzt** werden.*
- *Der Bund wird zudem sein Angebot an Kompetenzen und Werkzeugen zur Bekämpfung von Cyber-Kriminalität an die Länder **weiter ausbauen**.*
- *Um die Möglichkeiten zur Gefahrenabwehr bei Cyber-Angriffen zu verbessern, ist die Schaffung einer **erweiterten** Gesetzgebungs- und Verwaltungskompetenz des Bundes zur Abwehr von Gefahren zu prüfen.*

Die auf den Auf- und Ausbau sowie auf die Vertiefung und Erweiterung stützende Argumentationslinie zieht sich durch das gesamte Handlungsfeld. Was dagegen fehlt, ist die Bereitschaft, die bisherige Architektur zu entschlacken, zu straffen und effizienter zu organisieren. Ein Bürokratieaufbau verlangsamt nur wichtige Prozesse in der Cybersicherheit. Bitkom spricht sich dafür aus, bestehende Kompetenzen und Befugnisse zurückzunehmen, sofern die „strukturelle und prozessuale“ Bewertung dies begründet. Der erste Bullet Point ist entsprechend zu ergänzen. Die Analyse der noch durchzuführenden Bewertung darf dann natürlich nicht rein amtsintern stattfinden. Gleiches gilt für das Outsourcing der Verantwortung durch Verlagerung der Kontrolle in Allgemeinverfügungen, die z.T. verfassungs- und verwaltungsrechtliche Bedenken aufwerfen, wie es zuletzt Prof. Gärdiz in der Anhörung zum IT-Sicherheitsgesetz 2.0 unterstrichen hat. Verzerrte Interpretationsspielräume sind durch die Einbindung der Wirtschaft zu vermeiden. Eine gemeinsame Diskussion zur Interpretation der dann erfolgten Bewertung würde sich ebenfalls auf Ebene des Nationalen Cyber-Sicherheitsrats anbieten. An dieser Stelle sei auch auf unsere Ausführungen in Kapitel „5 Definition, Umsetzung und Controlling der Cyber-Sicherheitsstrategie“ verwiesen.

Einer der gelisteten Eckpunkte lautet: „*Die Digitale Souveränität soll **langfristig** in den Projekten zur konsolidierten IT des Bundes und zur konsolidierten Netzinfrastruktur des Bundes für eine sichere und zukunftsfähige Bearbeitung und Kommunikation besonders schutzbedürftiger Informationen berücksichtigt werden.*“ An dieser Stelle bedarf es eine Konkretisierung des Wortes „langfristig“.

Unklar ist zudem die neue Bund-Länder-Zusammenarbeit. Im Papier wird eher widersprüchlich die neue Zusammenarbeit skizziert. Teilweise erhält das BSI Befugnisse über neue Verträge der Zusammenarbeit und gleichzeitig sollen die Länder gestärkt werden. Hier gilt es eine balancierte Aufgabenverteilung zu finden, die nicht gegen die föderalen Strukturen verstößt. Die zukünftigen IT-Sicherheitsmaßnahmen bedürfen viele kompetente Einheiten. Die Länder können nicht nur auf die Aufklärung und Schadensbegrenzung reduziert werden, denn das BSI wird bundesweit kein Incident-Management betreiben können. Eine agile Struktur mit starken Partnern in den Ländern schafft erst eine flächendeckende „Cybersicherheits-Fürsorge".

Bitkom sieht den Eckpunkt: „*Um die technisch-operative Cyber-Sicherheit auf nationaler Ebene auch in der Detektion zukunftsfähig auszugestalten, sollten sich das Bundes Security Operations Center (BSOC) im BSI und die SOCs von Ländern und Wirtschaft in einem SOC-Verbund organisieren*." kritisch und hinsichtlich der Wirtschaft als zu weitgehend an. Hiermit würden sämtliche Unternehmen ausnahmslos dem BSOC des BSI untergeordnet. Daher ist zunächst eine grundsätzliche Diskussion über die Angemessenheit sowie dann zumindest eine Eingrenzung auf die vom IT-Sicherheitsgesetz regulierten KRITIS-Bereiche notwendig.

Bitkom empfiehlt zudem die Aufnahme und Ergänzung der folgenden Eckpunkte:

+ Neuer Eckpunkt:. *Die Cybersicherheitsstrategie sollte der Treiber für eine risikoorientierte Sicherheitsarchitektur sein. Diese setzt den Rahmen für eine innovative Beschaffung leistungsorientierter Technologien. Es gibt derzeit eine große Lücke zwischen dem Verständnis von Cybersicherheit und Beschaffungspraxis. In der Beschaffung kann zu oft von leistungsorientierten Bewertungskriterien abgewichen und bspw. der Schwerpunkt auf dem Preis gesetzt werden.*

## 4.4 Handlungsfeld 4 – Aktive Positionierung Deutschlands in der europäischen und internationalen Cyber-Sicherheitspolitik

Der erste Eckpunkt in Handlungsfeld 4 lautet: „*Die CSS 2021 soll inhaltliche Vorgaben europäischer Regelwerke zur Cyber-Sicherheit, wie insbesondere der NIS-Richtlinie, umsetzen und – soweit zeitlich bereits möglich und sachgerecht –Vorgaben aus dem Entwurf der NIS 2-Richtlinie berücksichtigen. Die CSS 2021 soll ein Verzeichnis enthalten, welches die Erfüllung europäischer Vorgaben für nationale Cyber-Sicherheitsstrategien nachvollziehbar macht. Auch die Cyber-Sicherheitsstrategie der EU für die digitale Dekade (EU-Cyber-Sicherheitsstrategie) ist zu berücksichtigen. Soweit die CSS 2021 Ziele der EU-Cyber-Sicherheitsstrategie aufgreift, soll dies an geeigneter Stelle in der CSS 2021 kenntlich*

*gemacht werden. In allen Handlungsfeldern der CSS 2021 sollen die europäischen Ziele in diesem Kontext auf nationale Ziele heruntergebrochen werden."*

Dieser Eckpunkt ist aus Sicht des Bitkom einer der erfolgskritischen Faktoren der CSS 2021. Bitkom betont nachdrücklich, dass ein europäisch einheitliches strategisches Vorgehen unabdingbar ist, um langfristig ein Höchstmaß an Cybersicherheit in Deutschland zu gewährleiten. Ein Divergieren künftiger nationalstaatlicher Cybersicherheitsstrategien muss um jeden Preis verhindert werden. Deutschland muss mit gutem Beispiel vorangehen und die deutsche CSS 2021 als Paradebeispiel für die Umsetzung der mit dem aktuellen Entwurf der NIS2-Richtlinie geforderten Anforderungen an eine nationalstaatliche CSS verstehen. Dazu sei nachfolgend die aktuelle Fassung des relevanten Passus aus dem Entwurf der NIS2-Richtlinie explizit angeführt. Wie auch immer die CSS 2021 letztendlich aussehen wird, die Strategie muss vor Verabschiedung an den neuen europäischen Vorgaben gespiegelt werden.

*Artikel 5 Nationale Cybersicherheitsstrategie des aktuellen NIS2-Entwurfs*

*(1) Jeder Mitgliedstaat verabschiedet eine nationale Cybersicherheitsstrategie, in der die strategischen Ziele sowie angemessene politische und regulatorische Maßnahmen zur Erreichung und Aufrechterhaltung eines hohen Cybersicherheitsniveaus festgelegt werden. Die nationale Cybersicherheitsstrategie muss insbesondere Folgendes umfassen:*

- *a) eine Beschreibung der für die Cybersicherheitsstrategie des jeweiligen Mitgliedstaats festgelegten Ziele und Prioritäten;*
- *b) einen Steuerungsrahmen zur Verwirklichung dieser Ziele und Prioritäten, der die in Absatz 2 genannten Konzepte sowie die Aufgaben und Zuständigkeiten öffentlicher Stellen und Einrichtungen sowie anderer relevanter Akteure umfasst;*
- *c) eine Bewertung zur Ermittlung von relevanten Anlagen und Cybersicherheitsrisiken in diesem Mitgliedstaat;*
- *d) die Bestimmung von Maßnahmen zur Gewährleistung der Vorsorge, Reaktion und Wiederherstellung bei Sicherheitsvorfällen, einschließlich der Zusammenarbeit zwischen dem öffentlichen und dem privaten Sektor;*
- *e) eine Liste der verschiedenen Behörden und Akteure, die an der Umsetzung der nationalen Cybersicherheitsstrategie beteiligt sind;*
- *f) einen politischen Rahmen für eine verstärkte Koordinierung zwischen den zuständigen Behörden im Rahmen dieser Richtlinie und der Richtlinie über die Resilienz kritischer Einrichtungen für die Zwecke des Informationsaustauschs über Sicherheitsvorfälle und Cyberbedrohungen und der Wahrnehmung von Aufsichtsaufgaben.*

*(2) Im Rahmen der nationalen Cybersicherheitsstrategie nehmen die Mitgliedstaaten insbesondere die folgenden Konzepte an:*

- *a) ein Konzept für die Cybersicherheit in der Lieferkette für IKT-Produkte und - Dienste, die von wesentlichen und wichtigen Einrichtungen für die Erbringung ihrer Dienste genutzt werden;*
- *b) Leitlinien für die Aufnahme und Spezifikation cybersicherheitsbezogener Anforderungen an IKT-Produkte und -Dienste bei der Vergabe öffentlicher Aufträge;*
- *c) ein Konzept zur Förderung und Erleichterung der koordinierten Offenlegung von Schwachstellen im Sinne des Artikels 6;*
- *d) ein Konzept im Zusammenhang mit der Aufrechterhaltung der allgemeinen Verfügbarkeit und Integrität des öffentlichen Kerns des offenen Internets;*
- *e) ein Konzept zur Förderung und Entwicklung von Cybersicherheitskompetenzen, Sensibilisierungsmaßnahmen sowie Forschungs- und Entwicklungsinitiativen;*
- *f) ein Konzept zur Unterstützung von Hochschul- und Forschungseinrichtungen bei der Entwicklung von Cybersicherheitsinstrumenten und sicherer Netzinfrastruktur;*
- *g) ein Konzept, einschlägige Verfahren und geeignete Instrumente für den Informationsaustausch, um den freiwilligen Austausch von Cybersicherheits-Informationen zwischen Unternehmen im Einklang mit dem Unionsrecht zu unterstützen;*
- *h) ein Konzept, das auf die spezifischen Bedürfnisse von KMU – insbesondere vom Anwendungsbereich dieser Richtlinie ausgenommener KMU – ausgerichtet ist und Orientierungshilfen sowie Unterstützung bei der Verbesserung ihrer Resilienz gegenüber Cybersicherheitsbedrohungen bietet.*

*(3) Die Mitgliedstaaten notifizieren der Kommission ihre nationalen Cybersicherheitsstrategien innerhalb von drei Monaten nach ihrer Verabschiedung. Die Mitgliedstaaten können bestimmte Informationen von der Notifizierung ausnehmen, wenn und soweit dies zur Wahrung der nationalen Sicherheit unbedingt erforderlich ist.*

*(4) Die Mitgliedstaaten bewerten ihre nationalen Cybersicherheitsstrategien mindestens alle vier Jahre auf der Grundlage wesentlicher Leistungsindikatoren und ändern diese erforderlichenfalls. Die Agentur der Europäischen Union für Cybersicherheit (ENISA) unterstützt die Mitgliedstaaten auf Anfrage bei der Entwicklung einer nationalen Strategie und wesentlicher Leistungsindikatoren für die Bewertung der Strategie.*

Bitkom weist darauf hin, dass zum Verständnis des Eckpunktes „*Der völkerrechtliche und normative Rahmen für den Cyber-Raum soll gestärkt, sowie auf ein international gemeinsames Verständnis über die Anwendung von Völkerrecht im Cyber-Raum und über verantwortliches Staatenverhalten hingewirkt werden*." eine klare Aussage für eine Verrechtlichung der Verantwortlichkeiten im Cyberraum, aber gegen jedwede Nationalisierung notwendig ist. So werden Staaten gestärkt, ohne neue Grenzen zu ziehen.

## 5 Definition, Umsetzung und Controlling der Cyber-Sicherheitsstrategie

Die Steuerung der CSS 2021 soll mittels eines strategischen Controllings durch das BMI sowie durch eine Begleitung der operativen Umsetzung durch die Ressorts erfolgen. Controlling sollte die Wirksamkeit der CSS 2021 daran messen, wie erfolgreich und schnell Deutschland digitalisiert wird. Sicherheit muss als Enabler verstanden werden und die Nutzung von IT als Chance für den Standort Deutschland. Die CSS2021 ist bspw. erfolgreich, wenn Schulen Unterstützung bei der Klärung der Rechtsunsicherheiten bei der Risikobewertung bekommen und diese nicht mehr auf der untersten Ebene individuell machen müssen.

Vor dem Hintergrund der Wichtigkeit des Zusammenspiels aus Digitalisierung und Cybersicherheit sowie der vielschichtigen Auswirkungen auf Staat, Wirtschaft und Bevölkerung stellt sich die Frage, ob die Gesamtverantwortung der Entwicklung der CSS 2021 bei nur einem Ressort liegen sollte. Aus unserer Sicht ist es zwingend erforderlich, dass Belange der Wirtschaft, Bildung (bspw. Homeschooling und digitale Ausgestaltung des Unterrichts an Schulen und Hochschulen), der Bevölkerung (sichere Nutzung digitaler Dienste), staatliche Sicherheitsinteressen (bspw. Prävention und Verfolgung von Straftaten) in einem ausgewogenen Verhältnis berücksichtigt werden. Dieses ausgewogene Verhältnis ließe sich besser erreichen, wenn das BMI die CSS 2021 in einem besonders partizipativen Prozess und im Sinne einer modernen Auslegung des Ressortprinzips zur Überwindung bestehender Silos mit den anderen wichtigen Häusern, insb. BMWi und BMBF, erstellt. Insofern regen wir eine Überarbeitung des Kapitels „4 Definition, Umsetzung und Controlling der Cyber-Sicherheits-Strategie" an, u.a. durch die Einführung einer vom Controlling abgegrenzten Gesamtergebniskontrolle.

Als Mitglied des Nationalen Cyber-Sicherheitsrats (NCSR), liegt für Bitkom eine Einbeziehung des NCSR in die Steuerung und Evaluierung der Cyber-Sicherheitsstrategie auf der Hand. Dass die enge Einbindung des NCSR im Eckpunktepapier nicht vorgesehen ist, erschließt sich Bitkom nicht.

Gemeinsam mit DIHK und BDI hat Bitkom unlängst in einem gemeinsamen Diskussionspapier zur Weiterentwicklung des NCSR dem BMI folgenden Vorschlag für das regelmäßige Monitoring der CSS 2021 unterbreitet: „*Der NCSR sollte jeweils in seiner Sommersitzung den aktuellen Umsetzungsstand der Nationalen Cyber-Sicherheitsstrategie 2021 beraten. Hierfür sollten die Bundesministerien rechtzeitig vor der Sitzung einen Umsetzungsreport erstellen und dem NCSR vorlegen. Die Wirtschaftsverbände BDI, Bitkom und DIHK bieten wiederum an, jährlich in ihrer Mitgliedschaft eine Umfrage zum aktuellen Umsetzungsstand (analog zur Umfrage zur CSS 2016) durchzuführen und die Ergebnisse in der Sommersitzung vorzustellen. Anschließend sollten die Mitglieder des NCSR dem Bundeskabinett einen Kurzbericht zum Umsetzungsstand der CSS 2021 auf Basis der vordefinierten Meilensteine vorlegen und darauf basierend Handlungsempfehlungen der Bundesregierung vorschlagen. Die wesentlichen Inhalte des Berichts sollten zudem in veröffentlichungsgerechter Form mit den Verbänden geteilt werden*.“

Bitkom wiederholt den Vorschlag, damit in den jährlichen Evaluierungsbericht zum Umsetzungsstand der CSS 2021 auch die Perspektive der Wirtschaft als entscheidender Akteur der deutschen Cybersicherheitsarchitektur einfließt.

Bitkom vertritt mehr als 2.700 Unternehmen der digitalen Wirtschaft, davon gut 2.000 Direktmitglieder. Sie erzielen allein mit IT- und Telekommunikationsleistungen jährlich Umsätze von 190 Milliarden Euro, darunter Exporte in Höhe von 50 Milliarden Euro. Die Bitkom-Mitglieder beschäftigen in Deutschland mehr als 2 Millionen Mitarbeiterinnen und Mitarbeiter. Zu den Mitgliedern zählen mehr als 1.000 Mittelständler, über 500 Startups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Geräte und Bauteile her, sind im Bereich der digitalen Medien tätig oder in anderer Weise Teil der digitalen Wirtschaft. 80 Prozent der Unternehmen haben ihren Hauptsitz in Deutschland, jeweils 8 Prozent kommen aus Europa und den USA, 4 Prozent aus anderen Regionen. Bitkom fördert und treibt die digitale Transformation der deutschen Wirtschaft und setzt sich für eine breite gesellschaftliche Teilhabe an den digitalen Entwicklungen ein. Ziel ist es, Deutschland zu einem weltweit führenden Digitalstandort zu machen.