VDE Stellungnahme

Stellungnahme zu den Eckpunkten einer Cyber-Sicherheitsstrategie 2021

Allgemeines und zu den Leitlinien:

- Es ist grundsätzlich sinnvoll, die bestehenden Handlungsfelder aus der CSS 2016 beizubehalten, da alle strategischen Ziele nach wie vor hierunter gefasst und entsprechende Erweiterungen innerhalb der jeweiligen Handlungsfelder platziert werden können.
- Zu begrüßen ist, dass der Begriff der „digitalen Souveränität“ als Leitlinie ausdrücklich in die CSS 2021 aufgenommen wurde und so aus einer bislang weitgehend konturlosen politischen Diskussion in konkrete Handlungsstränge überführt wird. Es sollte zur Herstellung digitaler Souveränität aber stärker auch auf privatwirtschaftliche Akteure referenziert werden, als es zurzeit vorgesehen ist. Digitale Souveränität wird primär durch technologische Innovation und nicht durch Gesetze und Regulierung gelebt.
- Es erschließt sich nicht ohne Weiteres, weshalb eine Leitlinie „Sichere Gestaltung der Digitalisierung“ durch die CSS 2021 vorgegeben werden soll. Auch wenn zwar unterschiedliche Akteure wie Staat, Wirtschaft und Gesellschaft angegeben werden, so stellt sich dennoch die Frage, weshalb eine solche Leitlinie gesonderter Erwähnung bedarf, da die CSS 2021 ohnehin auf eine „sichere Gestaltung der Digitalisierung“ ausgerichtet sein sollte.
- Die Messbarmachung von strategischen und gesetzlichen Zielen wird mittlerweile vielfach durch Wirtschaft und Zivilgesellschaft gefordert, insbesondere auch ausgelöst durch das Gesetzgebungsverfahren zum IT-SiG 2.0 und die dort vorgeschlagenen neuen Maßnahmen zur Cybersicherheit. Insoweit ist es begrüßenswert, dass auch in die CSS 2021 nunmehr Messbarkeitskriterien durch eine Leitlinie aufgenommen werden sollen (vgl. dazu auch Punkt 4 des Eckpunktepapiers CSS 2021). Unterschieden werden soll dabei zwischen „strategischen Zielen“ und „operativen Maßnahmen“. Insoweit bleibt zu hoffen, dass die zugrunde zu legenden Indikatoren auch in ihrer praktischen Anwendung hinreichend transparent sind. Zwar leuchtet das an dieser Stelle vorgeschlagene Ressortprinzip ein, jedoch wirkt es befremdlich, wenn sodann formuliert wird, dass „zur Steuerung und Überwachung der Umsetzung der Maßnahmen […] durch die Strategie keine Vorgaben gemacht […] werden.“ Hier sollten zumindest generelle Leitlinien vorgegeben werden.
- Eine stärkere Berücksichtigung von Normen und Standards ist angebracht, da diese einen wesentlichen Beitrag leisten können, u.a. wenn es darum geht, den Stand der Technik zu beschreiben und stetig zu aktualisieren, den „Security by Design“-Ansatz technisch umzusetzen und eine europaweite Harmonisierung von Anforderungen an IT-Sicherheit umzusetzen.

- Soweit Externe in die Evaluierung der CSS 2021 einbezogen werden, sollte durch Standardisierung der Abläufe deren Aufwand größtmöglich erleichtert werden, um umfassende Beteiligungsanreize zu schaffen.
- Soweit zur Steuerung der CSS 2021 ein transparentes Berichtswesen etabliert wird, ist dies zu begrüßen. Zumindest der Gesamtbericht über den Umsetzungsstand der CSS 2021 sollte der Öffentlichkeit zugänglich sein. Auch sollten die anlassbezogenen Evaluierungen veröffentlicht werden, um einen größtmöglichen Konsens im Hinblick auf die Umsetzung und eventuelle Anpassung der CSS 2021 zu erzielen.

Handlungsfeld 1 – Sicheres und selbstbestimmtes Handeln in einer digitalisierten Umgebung:

- Zu begrüßen ist weiterhin auch, dass zielgruppengerecht aufbereitete Informationsangebote gefördert werden sollen und dabei primär auch solche Akteure adressiert werden, die aufgrund begrenzter Ressourcen bislang nur schwer in der Lage gewesen sind, eigene Kapazitäten zu entfalten. Zu nennen sind hier neben Verbraucher*innen zuvorderst KMU, Bildungs- und Sozialeinrichtungen, Verbände und Vereine. Offen bleibt jedoch, was mit „staatlichen Angeboten des digitalen Verbraucherschutzes“ gemeint ist. Hier sollten entsprechende Beispiele genannt werden.
- Der EU-Binnenmarkt ist für die wirtschaftliche Entwicklung Deutschlands im neuen Jahrzehnt von zentraler Bedeutung. Mit der Digitalisierung geht der zunehmende Wunsch von Bürger*innen einher, dass entsprechende Produkte technisch sicher und datenschutzkonform sind. Richtigerweise wird deshalb das Ziel adressiert, in digitale, im EU-Binnenmarkt angebotene Produkte Aspekte der Cyber- und Informationssicherheit als Qualitätsmerkmal aufzunehmen. Inwieweit dies aber konform mit der aktuell sowohl in Deutschland als auch in der EU geführten politischen Debatte um die Aufhebung von Ende-zu-Ende verschlüsselter Kommunikation (Stichwort: „Sicherheit durch Verschlüsselung und Sicherheit trotz Verschlüsselung“) sein soll, erschließt sich nicht.
- Thematisiert wird die Einführung eines nationalen IT-Sicherheitskennzeichens, das auch Bestandteil der Ausführungen in der CSS 2016 gewesen ist. In welchem Zusammenhang dieses Kennzeichen zur Kennzeichnung nach dem aktuellen Entwurf des IT-SiG 2.0 stehen soll, erschließt sich nicht. Auch wird das deutsche freiwillige IT-Sicherheitskennzeichen kaum als „Engagement für die Einführung eines europaweit gültigen Kennzeichens mit verbindlichem Charakter“ gedeutet werden können. Inwieweit hier eine Passgenauigkeit zur EU Cyber-Sicherheitszertifizierung bestehen soll, geht aus den Erwägungen ebenfalls nicht hervor. Es sollte daher zwingend darauf geachtet werden, dass die nationale Cybersicherheitsgesetzgebung und die CSS 2021 in Einklang zueinander gebracht werden.
- Überdies ist es wichtig, die Funktionalität des NLF zu nutzen, um einen horizontalen Ansatz der europäischen Cybersicherheitsregulierung zu verfolgen. Ziel muss es hier sein, die CE-Kennzeichnung für die Anwendung bei Digitalprodukten und -anwendungen weiterzuentwickeln.
- Die Bezugnahme auf die deutsche Krypto-Strategie ist zu pauschal. Unklar ist, was unter einem „umfassenden Schutz“ für Bürger*innen und Wirtschaft/Institutionen vor Cyber-Gefahren zu verstehen sein soll und wie dies mit staatlichen Sicherheitsinteressen in Einklang zu bringen ist. Trügerisch wäre es, in der CSS 2021 eine Sicherheit zu signalisieren, die nach faktischer Gesetzeslage nicht besteht.
- Begrüßenswert ist die ausdrückliche Bezugnahme auf KI und IT-Sicherheit unter den zwei aktuell diskutierten Gesichtspunkten „IT-Sicherheit für KI und IT-Sicherheit durch KI“. Hinterfragt werden kann jedoch durchaus, ob die Nutzung von KI-Systemen handlungsfeldübergreifend unterzubringen bzw. zunächst zumindest stärker im B2B-Sektor zu verorten ist.
- Der im Eckpunktepapier angesprochene Ansatz „Netzwerke-schützen-Netzwerke“ hat sich bereits seit Jahren in der deutschen Cyber-Sicherheitsarchitektur bewährt und wurde schon vor der CSS 2016 in der Praxis gelebt. Dass dieser Ansatz in der CSS 2021 fortgeschrieben wird, ist deshalb nur konsequent. Jedoch ist auch hier festzustellen, dass der gegenwärtige Entwurf des IT-SiG 2.0 nicht in die Richtung einer Zusammenarbeit der relevanten Akteure auf Augenhöhe zusteuert, sondern vor allem einseitig Pflichten auferlegt, deren Notwendigkeit in verschiedenen Fällen nicht begründbar ist. Dies entspricht nicht einem Ansatz „Netzwerke-schützen-Netzwerke“.

- Cybersicherheit und illegitime Einflussnahme („Desinformation“) sind im digitalen Raum immer schwieriger voneinander zu trennen. Folgerichtig ist deshalb, dass im Handlungsfeld 1 auf die Informationsregulierung im Cyber-Raum abgestellt wird. Bei der Umsetzung entsprechender Maßnahmen muss jedoch im Lichte der Kommunikationsgrundrechte mit Augenmaß vorgegangen werden, soweit in Teilbereichen eine staatliche Regulierung angestrebt wird.
- Cybersicherheit als Qualitätsmerkmal „Made in Germany“: So begrüßenswert die digitale Souveränität auch sein mag – von einem Qualitätsmerkmal „Made in Germany“ zu sprechen, ohne auf das europäische Gesamtgefüge im Angesicht grenzüberschreitender Cyberbedrohungen abzustellen, ist hier verfehlt.
- Bezugnahme auf „Security by Design“: Die konsequente Umsetzung eines solchen Ziels schließt das Aufbrechen von Ende-zu-Ende-verschlüsselten Kommunikationswegen aus.

Handlungsfeld 2 – Gemeinsamer Auftrag von Staat und Wirtschaft:

- In der Einleitung der strategischen Ziele zum Handlungsfeld 2 heißt es: „Im Fokus dieses Handlungsfeldes steht daher die Zusammenarbeit zwischen Staat und Wirtschaft. In der CSS 2021 sollen der vertrauensvolle Austausch, das zeitnahe Schließen von Sicherheitslücken und die Abwehr von Cyber-Angriffen als unverzichtbare Bausteine des gemeinsamen Auftrags von Staat und Wirtschaft zur Erhöhung der Cyber-Sicherheit Deutschlands adressiert werden.“ Dass diese Ziele positiv zu würdigen sind, ist unbestritten. Auch hier stellt sich erneut jedoch die Frage, ob diese Ziele aktuell gesetzespolitisch konsequent umgesetzt werden, wenn beispielsweise festgestellte Sicherheitslücken zurückgehalten werden können.
- Cybersicherheit, Wirtschaftsschutz und unternehmerisches Engagement sind eine Grundvoraussetzung funktionierender Cybersicherheitsstrukturen. Ein derartiges Engagement, wie es von der CSS 2021 in den Eckpunkten gefordert wird, setzt jedoch Vertrauen voraus, soll eine funktionierende Zusammenarbeit mit staatlichen Einrichtungen stattfinden. Daher sollten Maßnahmen zur Stärkung dieses Vertrauens formuliert und umgesetzt werden.
- Zu begrüßen ist die Bezugnahme auf offene Basistechnologien, und auf offene und sichere Standards für Hard- und Software und deren Förderung.
- Auch nach wie vor ist es wichtig, KMU aktiv in die Gewährleistung von Cybersicherheit einzubeziehen. Entsprechender Weise schlägt das Eckpunktepapier vor, das Informationsangebot zur Unterstützung von Unternehmen bedarfsgerecht mit einem Fokus auf KMU auszubauen.
- Der Schutz von Kritischen Infrastrukturen ist ein zentraler Themenbereich im Handlungsfeld des gemeinsamen Auftrags von Staat und Wirtschaft. Zwar ist es wichtig, die rechtlichen Anforderungen an die sich regelmäßig ändernde Bedrohungslage anzupassen, jedoch sollte der Maßstab hierfür stets die Praktikabilität und der Mehrwert zusätzlicher Pflichten sein. Die gegenwärtige Formulierung einer „weiteren Ausgestaltung“ ohne Eingrenzung ist deshalb zu pauschal gewählt.
- Die Normung und Standardisierung werden in Handlungsfeld 2 detailliert aufgegriffen: Normen und Standards sollen zur Vermeidung von Doppelregulierung für Unternehmen im Bereich der Cybersicherheit EU-weit einheitlich definiert werden, die internationale Zusammen- und Gremienarbeit soll gestärkt werden und die internationale Wettbewerbsfähigkeit soll aufrechterhalten werden. Um Normen und Standards im Bereich Cybersicherheit 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.

Handlungsfeld 3 – Leistungsfähige und nachhaltige gesamtstaatliche Cyber-Sicherheitsarchitektur:

- Soweit eine strukturelle und prozessuale Bewertung der hochkomplexen Cybersicherheitsarchitektur des Bundes vorgeschlagen wird, sollte dafür Sorge getragen werden, dass die Ergebnisse einer solchen Bewertung auch den wissenschaftlichen und zivilgesellschaftlichen Akteuren zur Verfügung gestellt werden.
- Vorgeschlagen werden verschiedene Erweiterungen für den zwischenbehördlichen

Informationsaustausch und der Ausbau des BSI zur Zentralstelle im Bund-Länder-Verhältnis. So soll das BSI neben „BKA im Polizeiwesen und dem BfV im Verfassungsschutzverbund […] zur dritten Säule einer föderal integrierten Cyber-Sicherheitsarchitektur“ weiterentwickelt werden. Die gegenwärtigen Formulierungen nehmen nahezu ausschließlich auf Befugniserweiterungen des BSI und weitere Kompetenzen zur Datenübermittlung Bezug. Dabei unberücksichtigt bleiben aber die schon vielfach geäußerten datenschutzrechtlichen Bedenken, Cybersicherheit und die nicht selten betroffene informationelle Selbstbestimmung in Einklang zu bringen, und die Frage, ob und wie das BSI mit weiteren Sicherheitsbehörden kooperiert. Die Entwicklung einer leistungsfähigen und nachhaltigen gesamtstaatlichen Cybersicherheitsarchitektur steht nicht im leeren Raum, sondern ist vom Vertrauen der daran beteiligten wirtschaftlichen, wissenschaftlichen und zivilgesellschaftlichen Akteure abhängig.

- In der CSS geradezu sachfremd mutet es an, Maßnahmen zur Schwächung der Cybersicherheit vorzuschlagen, auch wenn diese – unter der grundsätzlich zulässigen Abwägung widerstreitender Interessen – gesetzlich generell möglich sein sollten. Das Zurückhalten von ermittelten Schwachstellen und die Schaffung von rechtlichen und technischen Möglichkeiten zur behördlichen Kompromittierung informationstechnischer Systeme sollten nicht Bestandteil der CSS sein. Insbesondere hier tritt der Interessenkonflikt, dem sich das BMI ausgesetzt sieht, besonders deutlich zutage.
- ZITiS hat den Auftrag, eigene Methoden und Werkzeuge zur Unterstützung der Sicherheitsbehörden zu entwickeln. Das Eckpunktepapier schlägt zusätzlich vor, dass falls kommerzielle Produkte zur Erfüllung der gesetzlichen Aufgaben von Polizeien und Nachrichtendiensten verwendet werden, „diese zur Erhöhung der Einsatzsicherheit möglichst umfassend geprüft werden sollen“. Die Formulierung lässt unberücksichtigt, dass der Rückgriff auf entsprechende kommerzielle Produkte ein Ausnahmefall bleiben sollte, und falls ein solcher Rückgriff stattfindet, eine vollumfängliche Überprüfung des Produkts zwingend sein muss und nicht eine bloße Sollvorgabe sein darf.
- Etwas kryptisch vorgeschlagen wird die „Untersuchung und Generierung von Prozessen für den Übergang von Cyber-Abwehr zu Cyber-Verteidigung bei komplexen Cyber-Lagen“. Da zum gegenwärtigen Zeitpunkt nicht erwiesen ist, ob Hack-back-Szenarien tatsächlich einen konkreten Mehrwert bieten und die Cybersicherheit gegebenenfalls sogar tendenziell eher schwächen, sollte davon abgesehen werden, diese Vorgabe in die CSS aufzunehmen. Auch dürfte fraglich sein, ob aktuell überhaupt eine Rechtsgrundlage zur Durchführung von Maßnahmen einer aktiven Cyber-Verteidigung im nationalen Recht verankert ist.
- Ob Open-RAN wie beispielhaft vorgeschlagen tatsächlich zu einer Stärkung der digitalen Souveränität beiträgt, ist umstritten. Nichtsdestotrotz ist es begrüßenswert, wenn allgemein offene Standards und interoperable Schnittstellen aktiv von staatlicher Seite gefördert und mit geeigneten Regulierungsansätzen begleitet werden.
- Welche konkrete Zielsetzung mit folgender Vorgabe aus dem Eckpunktepapier erreicht werden soll, erschließt sich nicht wirklich: „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.“
- Der Vorschlag zur Schaffung einer erweiterten Gesetzgebungs- und Verwaltungskompetenz des Bundes zur Gefahrenabwehr bei Cyber-Angriffen wirkt in der gegenwärtig vorliegenden Fassung noch zu unsubstantiiert und weit gefasst. So geht daraus nicht hervor, welche Behörden zu welchen Zwecken handeln sollen, um welche Arten von Cybergefahren es konkret geht und welche Ziele letzten Endes erreicht werden sollen. Insoweit wird auf die vorherigen Feststellungen zum Ausbau sicherheitsbehördlicher Kompetenzen in der Cybersicherheit verwiesen.

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

- Eine Angleichung der nationalen Cybersicherheitspolitik an die europäischen Vorgaben – dies sowohl strategisch mit Blick auf die Strategiepapiere als auch gesetzgeberisch mit Blick auf die EU NIS- und NIS 2-Richtlinie ist höchst sinnvoll, um insbesondere verpflichteten Unternehmen die Security-Compliance zu erleichtern und Mehraufwände zu

vermeiden. Auch hierzu ist aber gegenwärtig festzustellen: Der Vorschlag aus dem vorliegenden Eckpunktepapier und die tatsächliche Regulierung nach IT-SiG 2.0-E laufen noch auseinander. Eine klare Anschlussfähigkeit des nationalen Rechts an die europäischen Vorgaben ist aktuell nicht ohne Weiteres ersichtlich.

- Wie vorgeschlagen kann es sinnvoll sein, nationale Standards, Best Practices, etc. in europäische Regulierungen einfließen zu lassen. Auch hier darf aber nicht die EU-Perspektive außer Acht gelassen werden, denn es geht ebenso darum, von europäischer und mitgliedstaatlicher Ebene kommende und bewährte Ansätze in das nationale Regelwerk zu integrieren.
- Auch die neue EU-Cybersicherheitsstrategie aus 2020 greift die Themen Aufbau operativer Kapazitäten zur Prävention, Abschreckung und Reaktion auf. Mit Blick auf den „digitalen Gegenschlag“ stellen sich hier deshalb dieselben Probleme wie zuvor für den nationalen Rahmen formuliert. Hier sollten in Abstimmung mit den europäischen Vorgaben möglichst minimalinvasive Ansätze und Strategien verfolgt werden.

Ihre Ansprechpartner:

Markus B. Jaeger
Head of Political Affairs

VDE Verband der Elektrotechnik Elektronik Informationstechnik e.V.
Bismarckstraße 33, 10625 Berlin
Mobil +49 171 763 1986
markusb.jaeger@vde.com

Dipl.-Ing. (TU) Andreas Harner
Abteilungsleiter CERT@VDE & Cybersecurity

DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE
Stresemannallee 15, 60596 Frankfurt am Main
Mobil +49 151 628 557 76
andreas.harner@vde.com

Dr. Dennis-Kenji Kipker
Legal Advisor VDE Competence Center Information Security + CERT@VDE

DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE
Stresemannallee 15, 60596 Frankfurt am Main
Mobil +49 151 402 231 63
dennis-kenji.kipker@vde.com

Johannes Koch
Leiter Normungspolitik und Kooperationen

DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE
Stresemannallee 15, 60596 Frankfurt am Main
Mobil +49 170 188 7405
johannes.koch@vde.com