Anmerkungen zum Eckpunktepapier des Bundesministeriums des Innern, für Bau und Heimat „Eckpunkte für die Cyber-Sicherheitsstrategie 2021 (CSS 2021)“

Berlin, 14. April 2021

Mit der Cyber-Sicherheitsstrategie für Deutschland aus dem Jahr 2016 (CSS 2016) hat die Bundesregierung eine umfassende und systematische Grundlage für ihre Cybersicherheitspolitik gelegt. Die damaligen strategischen Überlegungen fokussierten sich dabei maßgeblich auf die neu eingerichtete Zentrale Stelle für Informationstechnik im Sicherheitsbereich (ZITiS) und die Rolle des Bundesamts für Sicherheit in der Informationstechnik (BSI). Nicht alle Aspekte der Cyber-Sicherheitsstrategie von 2016 waren unumstritten. Vor diesem Hintergrund schien die Evaluierung der damaligen Strategie im Jahr 2020 auch sinnvoll und begrüßenswert.

Mit dem nunmehr vorliegenden Eckpunktepapier zur Cyber-Sicherheitsstrategie 2021 zeigt das Bundesministerium des Innern, für Bau und Heimat (BMI), welche Schwerpunkte und Akzente von der nächsten CSS zu erwarten sind.

I. Allgemeine Anmerkungen

Nach Ansicht des eco ließ die Cyber-Sicherheitsstrategie aus dem Jahr 2016 zahlreiche Fragestellungen und Aspekte um den Umgang mit Verschlüsselung unbeantwortet. Das Credo von Sicherheitsbehörden „Sicherheit trotz Verschlüsselung“ war ein zentraler Kritikpunkt der damaligen Strategie, der aus der Sicht von eco die Zielsetzung der Cyber-Sicherheitsstrategie konterkariert hätte. Vor diesem Hintergrund kann eine abschließende Bewertung daher erst erfolgen, wenn die Fragestellungen und Aspekte um die Verschlüsselung beantwortet werden können und insbesondere nachdem geprüft wurde, inwieweit die Bundesregierung von diesem Ansatz abgekommen ist.

Die Erweiterung der Handlungsfelder um so genannte Leitlinien bewertet eco grundsätzlich positiv. Allerdings sollte darauf geachtet werden, dass die Strategie dadurch nicht insgesamt zu komplex wird und die geplante systematische Evaluierung auch unter diesem Aspekt und hinsichtlich der angedachten Erweiterung der Handlungsfelder handhabbar und praktikabel ist.

Vor dem Hintergrund, dass zahlreiche verschiedene Ressorts und Fachbereiche an der CSS 2021 beteiligt sind, stellt sich zudem die Frage, inwieweit eine Koordinierung an zentraler Stelle, bspw. im

Bundeskanzleramt, zweckmäßiger und sinnvoller wäre, als die vorgeschlagene Koordination durch das BMI, das sich dann mit den verschiedenen Ressorts abstimmen muss.

II. Zum Eckpunktepapier im Einzelnen

Zu: 2.1 „Handlungsfelder der CSS 2021“

Die vier im Eckpunktepapier der Bundesregierung angeführten Handlungsfelder für die CSS 2021 knüpfen an die CSS 2016 an. eco bewertet diese Anknüpfung und Fortschreibung als positiv. Die aufgezeigten Handlungsfelder setzen den richtigen Rahmen für die Pläne der Bundesregierung. Ihre Relevanz für die Gestaltung von IT-Sicherheit in Deutschland und Europa sind nach wie vor unverändert hoch.

Zu: 2.2 „Leitlinie Digitale Souveränität“

Das BMI hat in Aussicht gestellt, die Handlungsfelder der CSS 20221 um Leitlinien zu erweitern, die dann entsprechend auf die jeweiligen Handlungsfelder angewandt werden. Auf diese Weise wird eine Querschnittsbetrachtung angestrebt, die in den einzelnen Handlungsfeldern dann unterschiedlich stark ausgeprägt bewertet werden können. Für die jeweiligen Handlungsfelder werden für die einzelnen Leitlinien Schwerpunkte definiert. Die unter dem Aspekt der digitalen Souveränität angeführten Punkte bewertet eco positiv. Ergänzend hierzu würde eco begrüßen, wenn im Handlungsfeld 1 (Sicheres und selbstbestimmtes Handeln in einer digitalisierten Umgebung), neben der angewandten Forschung und deren Transfer, auch verstärkt die Unterstützung von Initiativen und Anwendungen wie GAIA-X berücksichtigt werden. So können neben IT-Sicherheit auch Datenschutz und digitale Souveränität gefördert werden.

Zu: 2.3 „Leitlinie Sichere Gestaltung der Digitalisierung“

Die sichere Gestaltung der Digitalisierung ist ein zentraler Baustein für das Vertrauen in digitale Technologien. Die hier dargelegte Leitlinie ist noch sehr abstrakt, so dass sich derzeit keine weiteren Ableitungen daraus ergeben. eco hält hier eine weitere Konkretisierung für sinnvoll. Insbesondere sollten Maßnahmen zur besseren Verbreitung von Verschlüsselungstechnologien und Unterstützung bei Security by Design Ansätzen in der Produkt- und Softwareentwicklung in den Leitlinien aufgegriffen und adressiert werden.

Zu: 2.4 „Leitlinie Effektivität und Messbarkeit der CSS 2021

eco begrüßt die Maßnahmen und Anregungen zur Messbarkeit der CSS 2021. Damit wird nicht nur für die jeweiligen Ressorts Klarheit über die Effektivität der angestrebten Ziele geschaffen, sondern darüber hinaus auch Transparenz gegenüber allen Beteiligten und der Zivilgesellschaft. Die Einbindung von Wirtschaft und Wissenschaft in die Evaluierung ist in diesem Kontext sinnvoll und sachgerecht. eco bewertet diesen dialogorientierten Ansatz für erfolgversprechend und unterstützenswert.

Zu: 3.1 „Handlungsfeld 1 – Sicheres und selbstbestimmtes Handeln in einer digitalisierten Umgebung“

Die unter dem Handlungsfeld 1 zusammengefassten Ziele bewertet eco positiv. Aufklärung, Information und begleitende Angebote sind ein wichtiger Aspekt und Baustein für den Aufbau von Vertrauen und den Erwerb von digitaler Kompetenz. Auch die Pläne zu sicheren elektronischen Identitäten sieht eco positiv. eco möchte in diesem Zusammenhang darauf hinweisen und zu bedenken geben, dass die Bemühungen im Rahmen der CSS 2021 und etwaig daraus resultierender Regulierung ebenfalls die aktuellen Entwicklungen hierzu auf europäischer Ebene einbeziehen sollten und auf die europäischen Ansätze Rücksicht genommen werden sollte. Die möglichen regulatorischen Vorgaben zur Gestaltung der Sicherheit in Telekommunikationsnetzen (mobil und leitungsgebunden) sollten mit Augenmaß getroffen werden und dürfen auf keinen Fall den wettbewerbsgetriebenen Ausbau von Netzen untergraben. Überlegungen zur Untersagung des Einsatzes bestimmter Technologie, ohne eine entsprechende Kompensation oder Entschädigung für bereits getätigte Investitionen durch den Staat, lehnt eco ab.

Zu: 3.2 „Handlungsfeld 2 – Gemeinsamer Auftrag für Staat und Wirtschaft“

Um das Niveau der IT-Sicherheit konsequent und nachhaltig zu verbessern, erfordert es nicht nur Anstrengungen von staatlicher Seite. Auch Anwender und Wirtschaft müssen hier einen Beitrag leisten. Vor diesem Hintergrund sind die Überlegungen im Bereich der Herausforderungen für Wirtschaft und Staat nachvollziehbar. Dennoch sollte nach Ansicht des eco insbesondere bei der zukünftigen Regulierung von kritischen Infrastrukturen (KRITIS) darauf geachtet werden, dass diese behutsam angepasst wird, da in diesem Bereich die Veränderung von Auflagen mit größeren Investitionen verbunden ist. Der mit der CSS vorgesehene Ansatz, die Aspekte der Marktzugangsregeln und Standards mit den aktuellen Entwicklungen und Vorhaben auf europäischer Ebene abzugleichen und darauf aufzubauen,

wird von eco ausdrücklich befürwortet und sollte dementsprechend weiterverfolgt und nicht durch nationale Alleingänge aufgegeben werden. Eine entsprechende Klarstellung dahingehend wäre in der CSS 2021 wäre begrüßenswert.

Dieser Ansatz sollte auch bei der Planung und Umsetzung von Cybersicherheitszertifikaten und Gütesiegeln entsprechend berücksichtigt und verfolgt werden.

Zu: 3.3 „Handlungsfeld 3 – Leistungsfähige und nachhaltige gesamtstaatliche Cyber-Sicherheitsarchitektur“

Die Cyber-Sicherheitsarchitektur hat sich in den vergangenen Jahren deutlich verändert. Konnte in Bezug auf die CSS 2016 noch konstatiert werden, dass Deutschland auf organisatorischer Seite relativ gut aufgestellt war, so hat sich in den vergangenen Jahren durch die stetige Einrichtung und Einbindung neuer und weiterer Einrichtungen, Gremien und Stellen mittlerweile eine Organisationsstruktur entwickelt, die immer komplexer und damit weniger praktikabel und handhabbar geworden ist. Vor diesem Hintergrund sollte eine Verschlankung der Cyber-Sicherheitsarchitektur in die Überlegungen einbezogen werden. Hierzu gehört eine dahingehende Überprüfung, inwieweit die Effizienz und Effektivität dadurch verbessert werden kann, dass die Anzahl der beteiligten Gremien und Stellen reduziert wird und auch inwieweit unter Umständen bestehende, sich überschneidende Kompetenzen und Zuständigkeiten eingeschränkt und bestenfalls sogar vermieden werden können. Diese Überlegungen sollten ebenfalls in die CSS 2021 mit einbezogen werden, da eine reine prozessorientierte CSS nach Ansicht des eco hier nicht ambitioniert genug wäre und aus Sicht der Internetwirtschaft nur wenig Verbesserung bringen würde.

Darüber hinaus sollte noch einmal deutlich gemacht werden, dass die Arbeit von ZITiS im Kontext der IT-Sicherheit nach wie vor problematisch ist und dementsprechend an dieser Stelle kein Beitrag zur Verbesserung der IT-Sicherheit durch diese Stelle zu erwarten ist. Daran ändert sich auch nichts durch die Anerkennung, dass diese Weiterentwicklung von ZITiS im Rahmen des geltenden Rechts zu erfolgen hat – insbesondere vor dem Hintergrund, dass mehrere Gesetze, die die Arbeit von ZITiS berühren, auch aus grundrechtlicher Sicht problematisch sind.

Zu: 3.4 „Handlungsfeld 4 – Aktive Positionierung Deutschlands in der europäischen und internationalen Cyber-Sicherheitspolitik“

Die CSS 2021 soll nach den Plänen des BMI in die europäische Politik eingefügt werden und die Auflagen von NIS und NIS 2 (soweit möglich)

berücksichtigen. eco begrüßt dieses Ansinnen und sieht ein harmonisiertes und nachvollziehbares Regulierungsgefüge, das europaweit möglichst einheitlich gestaltet und angewandt wird, positiv. Es sollte insbesondere darauf geachtet werden, dass die nationalen strategischen Ziele auf die europäischen Pläne einzahlen und nicht in einen Widerspruch zu diesen geraten.

III. Fazit

Die Eckpunkte für die CSS 2021 zeigen grundsätzlich positive Ansätze für deren weitere Ausgestaltung. In einzelnen Bereichen wäre eine grundlegendere Herangehensweise sinnvoll, die über die Optimierung von Prozessen und Abläufen hinausgeht und – einer echten Strategie folgend – einen konkreten Ansatz zur effizienteren Gestaltung von IT-Sicherheit und deren Regulierung bietet. Das institutionelle Gefüge der IT-Sicherheitsaufsicht und -regulierung ist in Deutschland zu komplex geworden und muss auch mit Blick auf eine europäische IT-Sicherheitsregulierung möglichst stringent und effizient ausgestaltet werden. Darüber hinaus sollte bei der CSS 2021 darauf geachtet werden, dass umstrittene Elemente, die in Widerspruch zu der strategischen Zielsetzung der Verbesserung von IT-Sicherheit stehen nicht in dieser Strategie angeführt werden. Die Arbeit von ZITiS und der Einsatz von Trojanern sollten dementsprechend nicht als strategisches Handlungsempfehlung oder strategisch wichtige Komponente angeführt werden. Eine dahingehende Klarstellung in der CSS 2021 wäre begrüßenswert.

Über eco

Mit über 1.100 Mitgliedsunternehmen ist eco der größte Verband der Internetwirtschaft in Europa. Seit 1995 gestaltet eco maßgeblich das Internet, fördert neue Technologien, schafft Rahmenbedingungen und vertritt die Interessen seiner Mitglieder gegenüber der Politik und in internationalen Gremien. Die Zuverlässigkeit und Stärkung der digitalen Infrastruktur, IT-Sicherheit und Vertrauen sowie eine ethisch orientierte Digitalisierung bilden Schwerpunkte der Verbandsarbeit. eco setzt sich für ein freies, technikneutrales und leistungsstarkes Internet ein.