VERBAND DER INTERNETWIRTSCHAFT E.V.

Eckpunkte zum Entwurf des Bundesministeriums des Innern, für Bau und Heimat zum Entwurf einer Cybersicherheitsstrategie für Deutschland (datiert auf: 9. Juni 2021)

Berlin, 30. August 2021

Mit der Cybersicherheitsstrategie schreibt die Bundesregierung die Schwerpunkte und Ziele für die Aktivitäten von Behörden und im Bereich der IT-Sicherheitspolitik fest. Eckpunkte der Cybersicherheitsstrategie 2021 (CSS21) hatte das Bundesministerium des Innern, für Bau und Heimat (BMI) bereits im April dieses Jahres veröffentlicht und beraten.

eco hat die Eckpunkte kommentiert und dargelegt, dass diese hilfreiche Ideen und Ansätze für eine Verbesserung der Cybersicherheit in Staat, Gesellschaft und Wirtschaft darstellen können, wenn sie richtig angewendet werden und keine weiteren Aspekte in die Strategie einfließen, die diese konterkarieren. Insbesondere sollte von Maßnahmen abgesehen werden, die eine systematische Ausnutzung von Schwachstellen in IT-Systemen durch Behörden als Beitrag zur Verbesserung der IT-Sicherheit vorsehen.

Am 9. Juni legte das BMI einen vorläufigen Entwurf für die CSS21 vor, der die Eckpunkte ergänzt und die adressierten Themen erweitert. Dieser Entwurf enthält mehrere Aspekte, die aus Sicht der Internetwirtschaft einer eingehenden Betrachtung bedürfen. In den nachfolgenden Eckpunkten geht eco auf diese Aspekte ein.

- **Zu 8.1.8 Verantwortungsvoller Umgang mit Schwachstellen – Coordinated Vulnerability Disclosure**

eco erachtet die unverzügliche Meldung von Schwachstellen, die Sicherheitsbehörden bekannt werden, an die jeweiligen Hersteller oder Entwickler als zentralen Faktor für die Verbesserung und Gewährleistung von IT-Sicherheit. Eine Strategie, die das systematische Zurückhalten von Sicherheitslücken vorsieht, insbesondere unter Einbeziehung des BSI, erachtet eco als äußerst kritisch. eco unterstützt die Bemühungen des BMI, Rechtssicherheit für Personen und Organisationen herzustellen, die Schwachstellen entdecken und diese melden.

- **Zu 8.3.1 Die Möglichkeiten des Bundes zur Gefahrenabwehr bei Cyberangriffen verbessern**

Die Möglichkeiten des Bundes zur Abwehr von Cyberangriffen sollen nach Plänen des BMI auch durch Grundgesetzänderungen ermöglicht und ausgebaut werden. eco warnt dringend davor, dass der Gesetzgeber hiermit

einen grundrechtssensiblen Bereich tangiert und damit auch Fernmeldegeheimnis aufgeweicht werden soll. Insbesondere sollte auch vorher abschließend geklärt werden, in welchem Umfang eine Gefahrenabwehr aufgefasst wird und unter welchen Voraussetzungen im Bereich der Gefahrenabwehr ermöglicht werden sollen.

- **Zu 8.3.7 Strafverfolgung im Cyberraum intensivieren**

eco erkennt an, dass die Strafverfolgung im Bereich der Kriminalität durch den Einsatz von IT ebenso wie die Strafverfolgung bei Angriffen auf IT intensiviert werden muss. eco erachtet dies als eine zentrale Herausforderung im Bereich der IT-Sicherheit, die der Staat in den kommenden Jahren angehen muss. Problematisch ist allerdings in den vorliegenden Formulierungen und Ausgestaltungen, dass der Staat dies nicht in einer sinnvollen, verhältnismäßigen und Grundrechte schonenden Weise adressiert. eco spricht sich eindeutig gegen den Einsatz von Trojanern in großem Umfang aus und fordert den Gesetzgeber dazu auf, weniger invasive Maßnahmen mit klaren Rechtsschranken zu entwickeln. Eine Mitwirkungspflicht der Unternehmen bei der Installation von Schadsoftware auf Endgeräten von Nutzer:innen lehnt eco ab.

- **Zu 8.3.8 Den verantwortungsvollen Umgang mit 0-day Schwachstellen und Exploits fördern**

eco erachtet die hier erörterte Frage nach einem richtigen Zeitpunkt zur Meldung von 0-day Schwachstellen als obsolet und nicht zielführend. Schwachstellen sollten durch öffentliche Stellen – sobald sie diesen bekannt werden – den jeweiligen Herstellern unverzüglich gemeldet werden. Gemeinsam mit den Herstellern sollte ein Weg zur umgehenden Beseitigung der Schwachstelle und damit der Minimierung der Risiken für Bürger:innen gesucht werden. Das Zurückhalten von Schwachstellen durch staatliche Behörden für andere Zwecke erachtet eco als verantwortungslos und konterproduktiv für die IT-Sicherheit. Behörden untergraben damit nicht nur die IT-Sicherheit sondern beschädigen auch das Vertrauen von Bürger:innen in staatliche Institutionen.

- **Zu 8.3.9 Sicherheit durch Verschlüsselung und Sicherheit trotz Verschlüsselung gewährleisten**

Einer der zentralen Kritikpunkte an der letzten Cybersicherheitsstrategie (CSS 2016) des Bundes waren die darin verankerten Ziele „Sicherheit durch Verschlüsselung“ und „Sicherheit trotz Verschlüsselung“. Nachdem in den bisherigen Beratungen der Eckpunkte der nunmehr vorliegenden

Sicherheitsstrategie diese Thesen nicht auftauchten, bestand Hoffnung, dass die Bundesregierung von diesem stark kritisierten Ansatz Abstand genommen hätte. Die nunmehr wieder aufgenommene Forderung hält eco für nicht akzeptabel. Die systematische Schwächung von Verschlüsselung – sei es durch das Ausnutzen von Sicherheitslücken oder gar durch Forderungen nach „Key Management“ oder „Zugangsmöglichkeiten“ – ist eine Gefährdung der Sicherheit, der Integrität und Vertraulichkeit der Kommunikation. Gerade vor dem Hintergrund, dass entsprechende Überlegungen im Entwurf der CSS 2021 vorkommen, stellt eco klar: Eine eingebaute Sicherheitslücke zur Umgehung von Verschlüsselung oder vergleichbare Lösungen stellt eine Gefahr für alle Nutzer entsprechender Geräte oder Software dar. Eine Mitwirkung von Herstellern oder Anbietern, wie die CSS 2021 sie zur Diskussion stellt, lehnt eco entschieden ab.

- **Zu 8.3.11 Die Digitale Souveränität der Sicherheitsbehörden durch den Ausbau der ZITiS stärken**

Bereits bei der Cybersicherheitsstrategie 2016 erachtete eco die Aufgaben und Funktion der Zentralen Stelle für die Informationstechnik im Sicherheitsbereich (ZITiS) als problematisch. Es war unklar, wie die ZITIS in IT-Systeme eindringt, welche Maßgaben und Verpflichtungen zum Schutz der Grundrechte alle Bürger dabei beachtet werden müssen. Die Cybersicherheitsstrategie 2021 sieht nun eine Ausweitung der Aufgaben und Befugnisse von ZITiS vor, obwohl diese zentralen Fragestellungen weiterhin nicht abschließend geklärt sind. eco plädiert hier für eine eingehende Prüfung der Aufgaben und Befugnisse von ZITiS und der rechtlichen Grundlagen, auf deren Basis ZITIS agiert.

- **Zu 8.3.12 Das Cybersicherheitsniveau durch gestärkte Vorfeldaufklärung erhöhen**

Die CSS2021 sieht eine Intensivierung der geheim- und nachrichtendienstlichen Aktivitäten vor. Vor dem Hintergrund der problematischen Erfahrungen der vergangenen Jahre und der jüngsten Gesetzgebung im Rahmen des BND-Gesetzes muss kritisch hinterfragt werden, inwieweit durch diese angedachte Intensivierung tatsächlich zu einer praktischen Verbesserung der IT-Sicherheitslage für Gesellschaft und Wirtschaft beitragen werden kann. eco plädiert für eine kritische Überprüfung der Ziele und Vorgaben für Geheimdienste und insbesondere für strengere Regeln bei Aktivitäten in Bezug auf TK-Netze und Internetinfrastrukturen.

- **Zu 8.3.14 Das Telekommunikations- und Telemedienrecht und die Fachgesetze an den technologischen Fortschritt anpassen**

eco sieht vor dem Hintergrund der voranschreitenden Digitalisierung Anknüpfungspunkte für eine Debatte um IT-Sicherheit in Zukunftstechnologien und den Zugang hierzu. Insbesondere auch im Rahmen der Diskussion um die digitale Souveränität ist dies relevant. Gleichzeitig warnt eco ausdrücklich davor, technologische Entwicklungen und Innovation, aktuellen tagespolitischen Erwägungen und Abwägungen zu unterwerfen.

- **Zu 8.4.6 Internationale Strafverfolgung stärken und internationale Cyberkriminalität bekämpfen**

Die Ausweitung und Verbesserung der grenzübergreifenden Strafverfolgung sieht eco als eine zentrale Herausforderung für die Ermittlungsbehörden an. Gleichzeitig existieren bei den bestehenden Ansätzen für die zukünftige Gestaltung einer solchen grenzübergreifenden Verfolgung von Straftaten enorme Probleme in Bezug auf den Schutz der Grundrechte von Bürgerinnen und Bürger, der Klärung der Territorialität von Straftaten – insbesondere im Bereich von Äußerungs- und Inhaltsdelikten – sowie die Rechtssicherheit für Unternehmen bei der Zusammenarbeit mit Strafverfolgungsbehörden. Bevor hier die Ausweitung von internationalen Übereinkünften angestrebt und der Zugriff von EU-Mitgliedsstaaten erweitert wird, sollte eine kritische Überprüfung stattfinden, so dass die hier angestrebten Ziele nicht durch staatliches Handeln konterkariert werden oder gar eine Schädigung bürgerlicher Rechte und Freiheiten nach sich ziehen.

- **Zu 8.4.7 Gemeinsam in der EU an innovativen Lösungen für eine effektivere Bekämpfung von Kriminalität arbeiten**

Wie bereits dargelegt erachtet eco die Arbeit von ZITiS als problematisch. Noch schwieriger stellt sich das in der CSS21 dargestellte Clearing Board auf europäischer Ebene (EuCB) dar. Es ist davon auszugehen, dass hier für Ermittlungs- oder auch geheimdienstliche Zwecke Erkenntnisse über Sicherheitslücken ausgetauscht werden sollen. Gerade vor dem Hintergrund der Weiterverbreitung von Informationen über das Vorliegen von Sicherheitslücken und Schwachstellen ist es aus Sicht der Internetwirtschaft fatal, wenn sich Bundesbehörden an einer solchen Proliferation beteiligen. eco erachtet die Idee des EuCB als gefährlich und rät dringend von weiteren Bemühungen in diesem Bereich ab.

Fazit

eco sieht eine Verbesserung der Cybersicherheit als zentrale Herausforderung für Staat, Gesellschaft und Wirtschaft und begrüßt, dass die Bundesregierung hier eine aktive Rolle einnimmt. Auch betrachtet eco eine Cybersicherheitsstrategie als zentralen Baustein für die Bundesregierung zur Wahrnehmung dieser Aufgabe.

Die Cybersicherheitsstrategie sieht eco als grundsätzlich gut und wichtig für die IT-Sicherheit in Deutschland. Sie legt Schwerpunkte und Zielsetzungen für längere Zeiträume fest und definiert strategische Ziele und Herausforderungen. In diesem Kontext befürwortet eco grundsätzlich, dass die Cybersicherheitsstrategie fortgeschrieben und auch in der kommenden Legislaturperiode die Schwerpunkte und Zielsetzungen im Bereich der der IT-Sicherheit festgelegt werden. Sie adressieren IT-Sicherheit als Querschnittsthema und bieten verschiedene Anknüpfungspunkte und Ansätze in verschiedenen Sektoren und Bereichen für Wirtschaft, Staat und Gesellschaft.

Bedauerlich ist allerdings, dass das BMI die Novellierung der CSS21 nicht genutzt hat, um der Strategie eine grundlegende Aktualisierung zu geben und das Ziel der Verbesserung der IT-Sicherheit durch fragliche Ziele und Ansätze im Bereich der Strafverfolgung und der Geheimdienstpolitik konterkariert. Aus der Sicht von eco müssen diese Probleme dringend adressiert und behoben werden. Nur so kann eine Verbesserung der IT-Sicherheit erreicht werden.

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.