VDA Verband der Automobilindustrie

Position

zur nationalen Cyber-Sicherheitsstrategie 2021

Berlin, April 2021

Ansprechpartner zum Thema

Geschäftsführung
Dr. Joachim Damasky

Abteilungsleiter
Matthias Krähling

Leiter Fachgruppe
Martin Lorenz
E-Mail: Martin.Lorenz@vda.de
Tel.: +49 (0) 30 897842-288

Allgemein

Im Verband der Automobilindustrie (VDA) haben sich über 600 Unternehmen der Branche – Hersteller von Kraftfahrzeugen und deren Motoren, Anhänger, Aufbauten und Container sowie Kraftfahrzeugteile und Zubehör – in Deutschland zusammengeschlossen, die als umsatzstärkste deutsche Industriebranche 2019 über 435 Mrd. Euro erwirtschaftete und mit rund 833.000 Mitarbeitern ca. 4,7 Mio. Pkw in Deutschland – von über 16 Mio. PKW weltweit – hergestellt hat. Hierzu sind die von unseren Mitgliedern erzeugten Nutzfahrzeuge (Lkw und Busse) hinzuzuzählen. Gemeinsam forschen und produzieren wir für eine saubere, sichere und nachhaltige Mobilität der Zukunft.

Der VDA begrüßt das Ziel, die Nationale Cybersicherheit zu stärken und die transparente Fortschreibung der Cyber-Sicherheitsstrategie (CSS) seit 2016 zu aktualisieren. Daten und somit auch die Cybersicherheit stehen seit Jahren im Mittelpunkt des täglichen Lebens und werden weiterhin unsere Zukunft in den Bereichen Politik, Verwaltung, Gesellschaft und Wirtschaft prägen. Die Gewährleistung und stetige Erhöhung der Cybersicherheit sind für die deutsche Automobilbranche ein essenzieller Bestandteil.

Gleichwohl bedürfen einige Eckpunkte für die Cyber-Sicherheitsstrategie 2021, aus Sicht des VDA, der Anpassung. Der aktuelle Entwurf beinhaltet die drei Leitlinien „Digitale Souveränität“, „Sichere Gestaltung der Digitalisierung“ und „Effektivität der Messbarkeit der CSS 2021“. Neben den drei Leitlinien wurden neue Ziele und Aspekte auf Ebenen von vier Handlungsfelder definiert. Hierbei handelt es sich um „Sicheres und bestimmtes Handeln in einer digitalisierten Umgebung“, „Gemeinsamer Auftrag von Staat und Wirtschaft“, Leistungsfähige und nachhaltige gesamtstaatliche Cyber-Sicherheitsarchitektur“ und „Aktive Positionierung Deutschlands in der europäischen und internationalen Cyber-Sicherheitspolitik.

Im Einzelnen:

Leitlinie „Digitale Souveränität“

Hierfür wird in der CSS 2021 die von IT-Rat und IT-Planungsrat abgestimmte Definition der Digitalen Souveränität zugrunde gelegt: Digitale Souveränität wird definiert als „die Fähigkeiten und Möglichkeiten von Individuen und Institutionen, ihre Rolle(n) in der digitalen Welt selbstständig, selbstbestimmt und sicher ausüben zu können“.

VDA-Position: Die Stärkung der Digitalen Souveränität ist für die deutsche Automobilindustrie ein zentrales Anliegen. Der Staat sollte bei erkannten Cyberangriffen gegen Unternehmen oder wichtige Einrichtungen die Digitale Souveränität stärken. Entsprechende Informationen und analysierte Bedrohungsmuster muss der Staat zeitnah mitteilen. Durch solche Maßnahmen sollen erkannte Schwachstellen rasch behoben werden. Sollten Indikatoren vorliegen, ob eine Schwachstelle von einem Angreifer bereits ausgenutzt wurde, muss dies ebenfalls mitgeteilt werden.

Somit kann ein besserer Austausch erzielt und die Stärkung der jeweiligen Digitalen Souveränität gewährleistet werden. Ein europäischer Austausch von Erkenntnissen zu Cyberangriffen würden die selbstbestimmten digitalen Werte besser schützen. Ebenso sollten auch staatliche Stellen bei Kenntnissen über Schwachstellen einer Informationspflicht unterliegen und diese Informationen nicht zurückhalten. Die Informationen bzw. Meldungen sollten koordiniert und vereinheitlicht werden, damit nicht an verschiedene Stellen verschiedene Infos gemeldet werden müssen. Digitale Souveränität kann nur existieren, wenn ein Höchstmaß an Cyberresilienz geschaffen wird. Die stetigen Beobachtungen zur Fortentwicklung der Cyber-Bedrohungen und ein Informationsaustausch sind unerlässlich.

Leitlinie „Sichere Gestaltung der Digitalisierung“

Diese Leitlinie soll die digitale Transformation von Staat, Wirtschaft und Gesellschaft vorantreiben. Die sichere Ausgestaltung ist Voraussetzung dafür, dass Digitalisierung souverän und zum Vorteil der Menschen in Deutschland gelingt.

VDA-Position: Der VDA begrüßt die Forderung einer sicheren Ausgestaltung der digitalen Transformation. Gleichwohl muss ein ausgewogenes Mittelmaß zwischen Cybersicherheit und wirtschaftlichem Fortschritt gefunden werden. Die Sicherheitslösungen müssen pragmatisch sein. Die Bundesregierung muss sich in Europa für starke Ende-zu-Ende-Verschlüsselung ohne Hintertüren einsetzen, um sensible Daten sowohl im privaten wie gewerblichen Kontext vor dem unberechtigten Zugriff Dritter zu schützen. Die sogenannten Hintertüren könnten zudem Angriffsmöglichkeiten für staatlich agierende Gruppen sowie für Kriminelle bieten. Aus diesem Grund spricht sich der VDA gegen die Schaffung von Hintertüren aus. Der Wirtschaftsschutz wird nicht durch Hintertüren gestärkt und Hintertüren schaffen keine Akzeptanz für das Label „Made in Germany“.

Leitlinie „Effektivität und Messbarkeit der CSS 2021“

Das Bundesinnenministerium erkennt an, dass zur Messbarmachung des Erfolgs der CSS 2021 auch messbare Ziele formuliert werden müssen.

VDA-Position: Die deutsche Automobilindustrie unterstützt dies mit Nachdruck. Hierzu wäre eine strukturierte Einbeziehung von Stakeholdergruppen bei der Umsetzung sowie kontinuierlichen Evaluation der CSS 2021 wünschenswert.

Handlungsfeld 1 – Sicheres und selbstbestimmtes Handeln in einer digitalisierten Umgebung

Der Anwendungsbereich des Handlungsfeld 1 soll das sichere und selbstbestimmte digitale Handeln von u.a. Bürgerinnen und Bürger, vom international agierenden Großkonzern über KMU, Verbänden bis hin zu Vereinen und Bildungseinrichtungen stärken. Gleichzeitig sollen staatliche Angebote des digitalen Verbraucherschutzes ausgebaut werden. Die CSS 2021 soll ebenfalls das Ziel adressieren, dass digitale Produkte und digitale Dienstleistungen, die im EU-Binnenmarkt angeboten werden, die Aspekte der Cyber- und Informationssicherheit als Qualitätsmerkmale beinhalten.

VDA-Position: Die schulische, berufliche und hochschulische Bildung bei der Digitalkompetenz sollte bundesweit gemäß einem Mindeststandard eingeführt werden. Voraussetzungen dafür ist die Digitalisierung an den Schulen und berufsbildenden Einrichtungen vorangetrieben wird und auch eine entsprechende Infrastruktur (Internetanbindung, WLAN, Notebooks / Tablets, Digitale Lernplattformen) zur Verfügung stehen. Weiterbildungsangebote müssen zumindest anwendungsbezogene Digitalkompetenzen enthalten und der Staat könnte Unternehmen, Verbände, Vereine usw. bei der Aus-/Fort-/Weiterbildung unterstützen.

Der Verbraucherschutz und Datenschutz sind in der vernetzten Digitalen Wirtschaft eine unaufhebbare Notwendigkeit. Aus diesem Grund sollte hier eine europäische Lösung geschaffen werden, der Cybersecurity Act bietet hier beispielsweise eine gute Grundlage. Die Einführung eines nationalen IT-Kennzeichens als Qualitätsmerkmal ist wenig hilfreich. Nur ein europaweit gültiges und europaweit einheitliches und leicht verständliches IT-Sicherheitskennzeichen (analog der UNECE R155) wird einen Beitrag zur Stärkung der Cybersicherheit voranbringen.

Handlungsfeld 2 – Gemeinsamer Auftrag von Staat und Wirtschaft

Die CSS hebt hervor, dass für die Cybersicherheit in Deutschland ein enger Austausch von Staat und Wirtschaft maßgeblich sei. Im Fokus des Handlungsfeldes 2 steht die Zusammenarbeit zwischen Staat und Wirtschaft. In der CSS 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.

VDA-Position: Der VDA begrüßt das Ansinnen zu mehr Cyber-Sicherheit, hierzu bedarf es einer einheitlichen Meldestruktur, die im Einklang mit dem IT-SIG 2.0 und der europäischen NIS 2 Richtlinie steht. Parallele Meldewege oder diverse formale Meldemuster schaffen keinen Mehrwert für die Cyber-Sicherheit.
Beim Erkennen von Bedrohungen müssen die Behörden mit dem jeweiligen Hersteller eines Produkts oder dem Anbieter einer Dienstleistung zusammenarbeiten und diese rechtzeitig vor jeder Offenlegung informieren. Die Hersteller müssen die Möglichkeit haben, ihren Kunden Updates oder Patches zur Verfügung zu stellen, um die Risiken der jeweiligen Sicherheitsanfälligkeit zu mindern, bevor eine Sicherheitsanfälligkeit von Dritten offengelegt wird. Andernfalls könnten Angreifer die offengelegten Schwachstellen ausnutzen und zum Nachteil der Cybersicherheit in Deutschland und Europa führen.

Handlungsfeld 3 – Leistungsfähige und nachhaltige gesamtstaatliche Cyber-Sicherheitsarchitektur

Der Staat muss Sicherheit, Recht und Freiheit in unserem Land auch im Cyber-Raum gewährleisten. Hierzu bedarf es einer zeitgemäßen Cyber-Sicherheitsarchitektur, die die verschiedenen Akteure auf Bundesebene wirksam verzahnt und daneben Länder, Kommunen und Wirtschaft im Blick behält.

VDA-Position: Der VDA fordert eine klare Struktur und feste Ansprechpartner bei den jeweiligen zuständigen Behörden. Ferner sollte hier ein Schulterschluss mit dem Wirtschaftsschutz geschlossen werden. Darüber hinaus sollten bestehende Gremien gestärkt werden, wie die Initiative Wirtschaftsschutz oder der Nationale Cyber-Sicherheitsrat und bei Bedarf könnten sogenannte Runde-Tische eingeführt werden. Ein regelmäßiger Erfahrungsaustausch zur Cybersicherheitsarchitektur und Infrastruktur zwischen Staat und den jeweiligen Unternehmensbranchen ist wünschenswert.

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

Ein hohes Niveau der Cyber-Sicherheit ist angesichts der transnationalen Vernetzung in einer digitalisierten Welt nur durch Einbettung der nationalen Maßnahmen in die entsprechenden europäischen, regionalen und internationalen Prozesse erreichbar. Während diese Einbettung in allen Handlungsfeldern mitbedacht werden muss, adressiert Handlungsfeld 4 diejenigen Ziele, für die sich Deutschland aktiv in die europäische und internationale Cyber-Sicherheitspolitik einbringen wird.

VDA-Position: Der VDA begrüßt die internationale Sichtweise zur Cyber-Sicherheitspolitik ausdrücklich. Durch den europäischen und internationalen Schulterschluss müssen Mehrfachregulierungen und redundante Berichtswege vermieden werden. Die nationalen Vorhaben müssen zumindest mit den europäischen Richtlinien und Vorhaben im Einklang stehen.

Definition, Umsetzung und Controlling der Cyber-Sicherheitsstrategie

Im Rahmen des Strategieprozesses zur CSS 2021 sollen grundlegende Strukturen für Umsetzung und Erfolgsmessung der Strategie dargelegt werden. Im Strategiedokument werden unter Ziffer 4.1 keine konkreten Maßnahmen zur Umsetzung dieser Ziele definiert, da die Entwicklung und Umsetzung individuell in der Hand der zuständigen Ressorts liegen. Maßnahmen werden nach abgeschlossener Erhebung in Form eines fortzuschreibenden Anhangs der Strategie beigefügt. Den Maßnahmen werden die verantwortlichen Ressorts zugeordnet.

VDA-Position: Eine Veröffentlichung konkreter Maßnahmen ist hochgradig sicherheitskritisch, da sich hieraus ein Security-Konzept ableiten lässt. Dies sorgt für eine Schwächung der Cyber-Sicherheit in der Wirtschaft.

Herausgeber Verband der Automobilindustrie e.V. (VDA)
Behrenstraße 35, 10117 Berlin
www.vda.de

Stand April 2021