VDA | Verband der Automobilindustrie

Position

Implementierung der NIS 2-Richtlinie in nationales Recht

Stärkung der Cyberresilienz in der EU

Berlin, März 2023

Einleitung

Die deutsche Automobilindustrie begrüßt den Abschluss der Trilogverhandlungen zur „Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rats vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148“ (NIS 2-Richtlinie). Im Zusammenspiel mit dem jüngst durch die EU-Kommission vorgeschlagenen Cyber Resilience Act sowie der ebenfalls bereits beschlossenen Resilience of Critical Entities Richtlinie wird die NIS 2 Europas digitale Resilienz nachhaltig stärken. Der VDA fordert die Bundesregierung auf, die NIS 2-Richtlinie rasch in nationales Recht zu überführen und den Wechselwirkungen der verschiedenen verwandten Regulierungen Rechnung zu tragen. Dabei gilt es, den Schutz vor digitalen und analogen Bedrohungen durch einen ganzheitlichen Ansatz zu erhöhen, die Kooperation von Staat und Wirtschaft zum Schutz des Industriestandorts Deutschland zu intensivieren, effiziente Prozesse aufzusetzen und risikoadäquate Anforderungen einzuführen. Des Weiteren sollte es bei der NIS 2-Umsetzung innerhalb der Europäischen Union eine weitgehend abgestimmte Überführung ins nationale Recht geben. Die deutsche Automobilindustrie ist stark in der Europäischen Union verzweigt und eine Stärkung der Cybersicherheit kann nur erreicht werden, wenn EU-weite einheitliche Rahmenbedingungen existieren.

In der jüngsten Vergangenheit sind zahlreiche Städte und Landkreise Opfer von weitreichenden Cybersicherheitsvorfällen geworden. Bürgerinnen und Bürgern sowie Unternehmen standen infolgedessen – teils über Monate – wichtige Verwaltungsdienstleistungen nicht zur Verfügung. Die deutsche Automobilindustrie ist auf eine stets gut funktionierende öffentliche Verwaltung, z.B. bei Planungs- und Genehmigungsverfahren, angewiesen. Angesichts der weitreichenden Ausweitung des Anwendungsbereichs der NIS 2 sind bereits mittlere Unternehmen mit mehr als 50 Mitarbeiterinnen und Mitarbeiter, respektive einem Jahresumsatz größer zehn Millionen Euro betroffen. Demnach müssen auch Kommunen, Landkreise und Städte zur Umsetzung von risikoadäquaten Cybersicherheitsmaßnahmen verpflichtet werden. Wir fordern die Bundesregierung auf, die Öffentliche Verwaltung aller Ebenen des Föderalstaats in den Anwendungsbereich aufzunehmen, damit alle Behörden risikoadäquate Cybersicherheitsmaßnahmen implementieren und so sensible Daten besser vor Cyberkriminellen schützen.

Unternehmenskategorien aus NIS 2 und IT-Sicherheitsgesetz 2.0 fusionieren

Im Sinne der Normenklarheit sollten im Rahmen der NIS 2-Umsetzung keine neuen Unternehmenskategorien eingeführt werden, sondern die sogenannten „essential entities“ und die „important entities“ mit den im deutschen Recht bestehenden Kategorien „Kritische Infrastrukturen“ und „Unternehmen im besonderen öffentlichen Interesse“ (UBI) fusioniert werden. Zudem sollten die Kategorien der Unternehmen im besonderen öffentlichen Interesse 1 bis 3 aufgelöst werden und zukünftig wieder ausschließlich Branchen maßgebend für die Aufnahme in das deutsche Umsetzungsgesetz sein. Die UBI 1 sollten als Branche zusätzlich zu den in der NIS 2 definierten Branchen in den Anwendungsbereich des Umsetzungsgesetzes aufgenommen werden.

Bei der Fusionierung des Anwendungsbereichs des deutschen und europäischen Cybersicherheitsrechts sind folgende Punkte zwingend zu beachten:

- Europäische Harmonisierung forcieren: Die Bundesregierung sollte bei der NIS 2-Implementierung sich so eng wie möglich am Anwendungsbereich der NIS 2 orientieren und keine darüberhinausgehenden Sektoren in Deutschland einführen/fortführen. (Sub-)Sektoren, die auf europäischer Ebene nicht als kritische Teilsektoren gelistet sind, sind aus dem Anwendungsbereich des NIS 2-Umsetzunggesetzes herauszunehmen. Dies würde beispielsweise den im BSIG existierenden Sektor Logistik betreffen, der aus europäischer Sicht richtigerweise in der NIS 2 nicht als eigenständige kritische Kategorie erachtet wird.

- Kompletter Wegfall von Anlagenbezogenen Schwellenwerten: Im Gegensatz zum bisher in der BSI-Kritisverordnung verfolgten Ansatz, Unternehmen nach der Anlagengröße dem Anwendungsbereich zuzurechnen, sollten zukünftig – gemäß NIS 2-Systematik – einzig die Unternehmensgröße (Zahl der Mitarbeiterinnen und Mitarbeiter sowie Jahresumsatz) ausschlaggebend sein.

- Nach Anhang 1, Ziff. 1 a) letzter Spiegelstrich zählen „Betreiber von Ladepunkten“ zu den wesentlichen Einrichtungen. Bei weiter Auslegung sind bereits Unternehmen als „wesentliche Einrichtung“ zu qualifizieren, wenn sie einen (1) Ladepunkt für ihre Mitarbeiter oder etwa für Kunden (beispielsweise Ladesäulen vor Supermärkten) betreiben. Es wären eine Vielzahl von Unternehmen erfasst; das kann ersichtlich nicht gewollt sein. Es sollte daher klargestellt werden, dass nur solche Unternehmen als wesentliche Einrichtungen zählen, deren primärer Geschäftszweck der Betrieb von Ladepunkten ist.

Berichtspflichten international und übergreifend abstimmen

Die NIS 2 beinhaltet eine Berichtspflicht für betroffene Unternehmen. Die nationale Implementierung der NIS 2 durch die 27 EU-Mitgliedstaaten kann zu einer mehrfachen, in Teilen verschiedentlichen Berichterstattung durch die Industrie gegenüber den nationalen Behörden führen. Die Bundesregierung sollte sicherstellen, dass Unternehmen nur in einem und nicht in allen EU-Mitgliedsstaaten berichten musst. Dies reduziert auch den Aufwand auf der Seite der nationalen Behörden, die ansonsten im internationalen Austausch die gleichen Informationen mehrfach erhalten und verarbeiten müssen.

Auf Basis der EU General Safety Regulation existiert bereits eine Berichtspflicht für die Automobilindustrie gegenüber nationalen Behörden. Die Bundesregierung sollte auch hier sicherstellen, dass eine Berichtspflicht über die gleichen Aspekte an verschiedene nationale Behörden vermieden wird.

Bußgeldrahmen nach Schwere der Ordnungswidrigkeit ausdifferenzieren

Bei der Einführung der neuen Bußgeldhöhen bedarf es einer deutlich feingranulareren und an Ordnungswidrigkeiten angepasste Bußgeldhöhen als dies durch die pauschalen Obergrenzen nach Artikel 34 Nummer 3 und 4 in der NIS 2-Richtlinie angelegt ist. Der VDA stimmt grundsätzlich der Einführung von Bußgeldern zur Ahndung der Nichteinhaltung rechtlicher Anforderungen zu. Allerdings sollte die Höhe von Bußgeldern stets proportional zu Ordnungswidrigkeit sein. Zudem müssen mehrfache Bußgelder (e.g. aufgrund DSGVO, sowie NIS 2-Verletzung) für gleiche Versäumnisse weiterhin ausgeschlossen sein.

Hohe Strafen gegenüber betroffenen Unternehmen wirken bezüglich des Schaffens von Transparenz über aktuelle Angriffsvektoren kontraproduktiv. Insofern sollten die für das Strafrecht entwickelten Grundsätze bei der Bemessung der Strafe auf Ordnungswidrigkeiten im hier behandelten Zusammenhang übertragen werden.

Sicherheitsanforderungen, wie CSA-Schema, europaweit einheitlich einführen

Damit NIS 2 seine volle Wirkung entfalten kann, fordern wir die Bundesregierung zu einer möglichst engen Abstimmung mit ihren europäischen Partnern bei der Definition von Sicherheitsmaßnahmen auf. Zahlreiche essential und important Entities sind nicht nur grenzüberschreitend tätig, sondern sind Teil eines größeren Ökosystems mit gegenseitigen Abhängigkeiten entlang der Wertschöpfungskette. Viele ihrer Anbieter erbringen Dienstleistungen, die in mehreren Sektoren angeboten werden. Daher sollten die nationalen Regierungen im Rat die Umsetzung der NIS 2 bestmöglich abstimmen. Durch ein Höchstmaß an europaweiter regulatorischer Konsistenz kann die Cyberresilienz der gesamten EU nochmals gestärkt werden. Zugleich können so Effizienzgewinne bei der Implementierung durch Unternehmen gehoben werden.

Risikoadäquat cyberresiliente Produkte sind eine zentrale Voraussetzung für die Umsetzung technischer Cybersicherheitsmaßnahmen. Daher unterstützt der VDA ausdrücklich die Einführung von horizontalen Cybersicherheitsanforderungen für Produkte mit digitalen Elementen sowie eines Schwachstellenmanagements im Rahmen des Cyber Resilience Acts (CRA).

Gleichwohl sollte wie im CRA auch in der NIS 2-Richtlinie Fahrzeuge gemäß der Verordnung (EU) 2019/2144 [über die Anforderungen für die Typgenehmigung von Kraftfahrzeugen und Kraftfahrzeuganhängern, und Systeme, Bauteile und selbstständige technische Einheiten für diese Fahrzeuge] ausgenommen werden.

Für Fahrzeuge bestehen heute bereits mindestens gleichwertige Cybersecurity Anforderungen nach Verordnung (EU) 2019/2144 [über die Anforderungen für die Typgenehmigung von Kraftfahrzeugen und Kraftfahrzeuganhängern, und Systeme, Bauteile und selbstständige technische Einheiten für diese Fahrzeuge]. Es sollte daher klargestellt werden, dass, auch in der NIS 2-Richtlinie, wie in der CRA, die Verordnung (EU) 2019/2144 als „sector-spezifische“ Regulierung anerkannt wird und die Anforderungen der NIS 2 (IT-SicherheitsG. 3.0) nicht für Fahrzeuge und -dienste gelten.

Möglichkeit zur Überprüfung der Vertrauenswürdigkeit der Beschäftigten schaffen

Der Schutz vor digitalen Risiken gelingt nur im Zusammenspiel von technischen, organisatorischen und personellen Maßnahmen. Die weitreichenden organisatorischen, operativen und technischen Maßnahmen, die wesentliche und wichtige Einrichtungen gemäß Artikel 21 NIS 2-Richtlinie, zukünftig zur Stärkung ihrer Cyberresilienz implementieren müssen, werden ins Leere laufen, wenn sie durch Mitarbeitende – ganz gleich welcher Herkunft – ausgeführt werden, die dem Unternehmen schaden wollen/sollen. Um die Gefahr des Innentäters zu minimieren und die Wirksamkeit organisatorischer, operativer und technischer Cybersicherheitsmaßnahmen zu erhöhen, sollten im Sinne eines umfassenden und vorausschauenden Wirtschaftsschutzes Sicherheitsüberprüfungen auch für Unternehmen möglich sein, die keine sicherheitsbetreuten Unternehmen im Sinne des Sicherheitsüberprüfungsgesetzes (SÜG) sind. Zukünftig sollten alle Unternehmen, die dem Anwendungsbereich des NIS 2-Umsetzunggesetzes unterliegen, die Möglichkeit erhalten, bei den zuständigen Stellen eine Sicherheitsüberprüfung für Mitarbeitende zu beantragen, die in sicherheitsrelevanten Funktionen tätig sind. Die Bundesregierung muss zwingend eine entsprechende KANN-Möglichkeit im Rahmen des NIS 2-Umsetzunggesetzes einführen. Eine ausschließliche Fokussierung auf technische Sicherheit ist nicht zielführend. Unternehmen sollten auch die Möglichkeit erhalten, die Vertrauenswürdigkeit von Beschäftigten und Bewerbern, die in besonders sicherheitskritischen Bereichen tätig sind, untersuchen zu können. Es müssen zukünftig auch Verfahren geschaffen werden, mit denen ausländische Mitarbeiter in die Prüfung einbezogen werden können. Auch sind die Prozesslängen zu verkürzen. Mehrmonatige Wartezeiten, wie sie aktuell in der Sicherheitsüberprüfung vorkommen, hemmen die Wirtschaft und tragen nicht zur Sicherheit bei.

UP KRITIS um Vertreterinnen und Vertreter von essential und important Entities zu ergänzen

Alle Unternehmen, die zukünftig als wesentliche und wichtigen Einrichtungen in den Anwendungsbereich der deutschen Cybersicherheitsgesetzgebung aufgenommen werden, sollten die Möglichkeit zur Teilnahme am Umsetzungsplan KRITIS (UP KRITIS) erhalten. Durch die strukturierte Einbindung der neu in den Anwendungsbereich der Cybersicherheitsgesetzgebung fallenden Unternehmen in den UP KRITIS kann der Austausch zu aktuellen Sicherheitsvorfällen sowie zur Umsetzung der technischen und organisatorischen Maßnahmen deutlich verbessert werden. Auch müssen Herstellern von Produkten und Systemen, die von wesentlichen Einrichtungen eingesetzt werden, deutlich besser in diese Gesprächsformaten eingebunden werden.

Stand der Technik durch die Wirtschaft entwickeln lassen und nicht gesetzlich definieren

Die Festlegung des „Standes der Technik“ und darauf basierend der Erlass von Durchführungsakten sollte auch zukünftig nicht der EU-Kommission oder nationalen Behörden obliegen. Vielmehr müssen von der Wirtschaft erarbeitete anerkannte Normen, Standards und Spezifikationen sowie bewährte branchenspezifische Regelungen der Automobilindustrie implementiert werden. Diese werden durch die betroffenen Fachkreise ständig aktualisiert und entsprechen damit dem realen Stand der Technik – eine regulatorische Anforderung könnte dies aufgrund langwieriger Verwaltungsverfahren niemals in gleicher Weise widerspiegeln. Zudem gehen die so entwickelten Anforderungen an den Stand der Technik bereits mit Umsetzungsanweisungen und -vorschriften einher. Nur dadurch sind die notwendige Flexibilität und Reaktionsgeschwindigkeit auf Veränderungen gesichert.

Weitere Implementierung des IT-Sicherheitsgesetzes 2.0 aussetzen

Angesichts der zeitnahen Umsetzung der NIS 2-Richtlinie in nationales Recht, sollte die Bundesregierung die weitere Implementierung noch nicht umgesetzter Anforderungen aus dem IT-Sicherheitsgesetz 2.0 aussetzen. Insbesondere sollte die Bundesregierung die Einführung der Unternehmen im besonderen öffentlichen Interesse der Kategorie II (inländische Wertschöpfung und deren Zulieferer, UBI 2) nach Paragraf 2 Absatz 14 (2) nicht weiter forcieren. Dem zusätzlichen Erfüllungsaufwand, der sich für die betreffenden Unternehmen aus einer konsekutiven Implementierung von Paragraf 8f BSIG sowie der NIS 2 ergeben würde, steht in keinem Verhältnis zur sich daraus ergebenden marginalen Stärkung der Cyberresilienz.

Bereitstellung von und Rechtsrahmen zu Umsetzungs-/ Orientierungshilfen

Im Rahmen der NIS 2-Richtlinie, bzw. im Kontext der Transformation dieser in nationales Recht, sollten vom Gesetzgeber zeitnah ausreichend konkrete Umsetzungs-/Orientierungshilfen zum Gesetz bereitgestellt werden. Diese sollten im besten Fall parallel mit dem Inkrafttreten des neuen lokalen NIS 2-Umsetzungsgesetzes bereitgestellt werden. Des Weiteren ist der Rechtsrahmen dieser eindeutig zu klären. D.h. es muss für die betroffenen Entitäten klar sein, ob diese lediglich Hilfen/Orientierungen darstellen, oder ob diese rechtsverbindlich und vollumfänglich umgesetzt werden müssen. Im heutigen DE KRITIS-Umfeld existieren zwar solche Umsetzungs-/Orientierungshilfen, es ist jedoch nicht klar, ob diese für die betroffenen Unternehmen rechtsverbindlich sind.

Effizientes, volldigitalisiertes Registrierungs- und Meldewesen etablieren

Um die sich aus Artikel 23 der NIS 2-Richtlinie ergebenden Erfüllungsaufwände mit Blick auf die Registrierungs- und Meldung von Vorfällen in einem vertretbaren Rahmen zu halten, bedarf es der Einführung eines effizienten, volldigitalisierten Registrierungs- und Meldewesens auf Basis des Once-Only-Prinzips. Bereits seit dem IT-Sicherheitsgesetz müssen Unternehmen, die als Betreiber kritischer Infrastrukturen definiert werden, sich beim BSI registrieren. Diese Anforderung wurde mit dem IT-Sicherheitsgesetz 2.0 auf Unternehmen im besonderen öffentlichen Interesse ausgeweitet. Mit der NIS 2- und der Resilience-of-Critical-Entities-Richtlinie werden sich zukünftig noch weitere Unternehmen beim BSI registrieren müssen, zahlreiche davon zusätzlich beim Bundesamt für Bevölkerungs- und Katastrophenschutz. Diese Registrierungspflichten sollten im Sinne einer nutzendenorientierten öffentlichen Verwaltung in einen effizienten und volldigitalisierten Prozess zusammengeführt werden. Auf die so gemeldeten Registrierungsdaten sollten die zuständigen staatlichen Stellen nach dem Need-to-Know-Prinzip zugreifen können. Dies würde die Erfüllungsaufwände reduzieren, Registrierungen zentral korrelieren und in den betroffenen Unternehmen Kapazitäten schaffen, um den Schutz vor Bedrohungen zu erhöhen.

Auch beim Meldewesen braucht es dringend ein effizientes, volldigitalisiertes Verfahren, um relevante Incidents zentral, einheitlich und korreliert zu erfassen. Die NIS 2-Richtlinie sieht vor, dass Unternehmen zukünftig mindestens drei und bis zu fünf Meldungen pro Cybersicherheitsvorfall vornehmen sollen. Wir fordern die Bundesregierung auf, gemeinsam mit der Wirtschaft ein Meldewesen zu etablieren, über das Unternehmen direkt all ihren Meldeverpflichtungen, die sich aus der NIS 2- und der RCE/CER-Richtlinien – aber auch aus aktuell schon bestehenden fachspezifischen Meldepflichten – ergeben, erfüllen können. Alle zuständigen Behörden auf Bundes-, Länder- und Kommunal-Ebene – darunter das Bundesamt für Sicherheit in der Informationstechnik, das Bundesamt für Bevölkerungs- und Katastrophenschutz sowie die Kriminalämter und Polizeien auf Bundes- und Landesebene – sollten nach dem Need-to-Know-Prinzip Zugang zu den so gemeldeten Informationen erhalten. Daneben muss die Bundesregierung in Abstimmung mit den weiteren Mitgliedsstaaten der Europäischen Union sicherstellen, dass Unternehmen, die in den Anwendungsbereich von Artikel 26 fallen, nur in einem Mitgliedsstaat entsprechende Cybersicherheitsvorfälle melden müssen. Die Mitgliedsstaaten sollten untereinander in geeigneter Form einen Informationsfluss über entsprechende Vorfälle sicherstellen, ohne dass dadurch den betroffenen Wirtschaftsakteuren Mehraufwände entstehen. Dies ist von besonderer Bedeutung für die Unterkategorie der nummernunabhängigen interpersonellen Kommunikationsdienste (NI-ICS) der öffentlich

zugänglichen elektronischen Kommunikationsdienste gemäß Artikel 26 Absatz 1 (a). Diese Dienste werden über das Internet bereitgestellt und sind in der Regel europaweit verfügbar. Als solche haben sie viel mit den über digitalen Infrastrukturen und digitalen Anbietern in Abschnitt 8 von Anhang I und Abschnitt 6 von Anhang II gemeinsam. Im Gegensatz zu diesen Anbietern richtet sich die Zuständigkeit jedoch nicht nach der Hauptniederlassung in der EU, sondern danach, wo sie ihre Dienstleistungen erbringen. Als solche unterliegen sie wahrscheinlich 27 verschiedenen Registrierungs- und Meldepflichten anstelle einer einzigen. In der Kooperationsgruppe sollten Anstrengungen unternommen werden, um sicherzustellen, dass solche Anbieter nur einer einzigen Stelle Bericht erstatten müssen, wobei ein zusätzlicher Informationsaustausch zwischen den Mitgliedstaaten erfolgen sollte.

Ferner sollten Unternehmen im Rahmen von Folge-Meldungen immer auf die bereits gemeldeten Informationen zugreifen und diese anreichern und korrigieren können, statt immer von Null beginnen zu müssen. Zudem sollten das BSI und die Computer Security Incident Response Team (CSIRTs) nur in herausgehobenen Fällen einen Zwischenbericht nach Artikel 24 23 Absatz 4 (c) einfordern. Angesichts der Ausweitung des Anwendungsbereichs auf mittlere Unternehmen und des zugleich existierenden massiven Fachkräftemangels an IT-Security-Expertinnen und -Experten, werden ohne einen einheitlichen und schlanken digitalen Meldeweg zahlreiche Unternehmen den entsprechenden Verpflichtungstatbeständen nicht innerhalb der rechtlich definierten Fristen nachkommen können.

Über uns

Der Verband der Automobilindustrie (VDA) vereint mehr als 650 Hersteller und Zulieferer unter einem Dach. Die Mitglieder entwickeln und produzieren Pkw und Lkw, Software, Anhänger, Aufbauten, Busse, Teile und Zubehör sowie immer neue Mobilitätsangebote. Wir sind die Interessenvertretung der Automobilindustrie und stehen für eine moderne, zukunftsorientierte multimodale Mobilität auf dem Weg zur Klimaneutralität. Der VDA vertritt die Interessen seiner Mitglieder gegenüber Politik, Medien und gesellschaftlichen Gruppen. Wir arbeiten für Elektromobilität, klimaneutrale Antriebe, die Umsetzung der Klimaziele, Rohstoffsicherung, Digitalisierung und Vernetzung sowie German Engineering. Wir setzen uns dabei für einen wettbewerbsfähigen Wirtschafts- und Innovationsstandort ein. Unsere Industrie sichert Wohlstand in Deutschland: Mehr als 780.000 Menschen sind direkt in der deutschen Automobilindustrie beschäftigt. Der VDA ist Veranstalter der größten internationalen Mobilitätsplattform IAA MOBILITY und der IAA TRANSPORTATION, der weltweit wichtigsten Plattform für die Zukunft der Nutzfahrzeugindustrie.

Ansprechpartner

Dr. Marcus Bollig
Geschäftsführung
marcus.bollig@vda.de

Martin Lorenz
Abteilungsleiter (komm.) Fahrzeugtechnologien & Eco-Systeme Fachgebietsleiter Security & Daten
martin.lorenz@vda.de

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

Registrierter Interessenvertreter R001243
EU-Transparenzregister-Nr. 95574664768-90

Version
Version 1.0, März 2023