VDA Verband der Automobilindustrie

Position

Cybersicherheit

NIS 2-Richtlinie der Europäischen Union

Berlin, März 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 der Europäischen Kommission, die Cybersicherheit in Europa deutlich zu stärken und faire Wettbewerbsbedingungen in der Europäischen Union zu schaffen. 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 ist für die gesamte Europäische Union essenziell. Gerade die zunehmenden Verflechtungen zwischen Sektoren und Akteuren und entlang der Lieferketten sind von immenser Bedeutung. Daher begrüß der VDA den Vorschlag der EU-Kommission zur Aufhebung der Richtlinie (EU) 2016/1148 und den Vorschlag einer Richtlinie über Maßnahmen zur Cybersicherheit in der gesamten Union (NIS2-Richtlinie) als einen wichtigen Schritt in die richtige Richtung. Die NIS 2-Richtlinie enthält 84 Erwägungsgründe und ist in sieben Kapitel unterteilt. Die Kapitel befassen sich mit allgemeinen Bestimmungen, Koordinierte Rechtsrahmen für die Cybersicherheit, Zusammenarbeit, Risikomanagement und Meldepflichten im Bereich Cybersicherheit, Informationsaustausch, Aufsicht und Durchsetzung sowie Übergangs und Schlussbestimmungen.

Gleichwohl bedarf die NIS 2-Richtlinie, aus Sicht des VDA, einige Anpassung und der VDA fordert die EU-Kommission, das Europäische Parlament und die Mitgliedstaaten auf, diese Bemerkungen während des Gesetzgebungsverfahrens zu prüfen. Sofern an diesem Entwurf festgehalten wird, könnten gemäß der Empfehlung 2003/361/EG über 500 Unternehmen der deutschen Automobilbranche unter diese Regelung fallen. Durch den hohen Anwendungsbereich der NIS 2-Richtlinie werden viele Unternehmen zusätzlichen Belastungen ausgesetzt. Diese zusätzlichen Belastungen können zu einem Wettbewerbsnachteil führen, insbesondere beim Vergleich mit Unternehmen aus Drittstaaten.

Im Einzelnen:

Verschlüsselung (Nummer 54)

Die NIS 2 Richtlinie soll gemäß dem Erwägungsgrund Nummer 54 die Verwendung von Ende-zu-Ende-Verschlüsselung fördern, und für Unternehmen bindend einführen. Die Ende-zu-Ende Verschlüsselung soll zudem den Behörden die Möglichkeit bieten, Zugang zu diesen Informationen für strafrechtliche Ermittlungen zu ermöglichen.

VDA-Position: Der VDA fordert die Europäische Kommission, das Europäische Parlament und die EU-Mitgliedstaaten auf, eine notwendige Verschlüsselung zu fördern, jedoch sollen die kryptografischen Verfahren nicht geschwächt werden. Die deutsche Automobilindustrie unterstützt die zuständigen Behörden bei der Erhebung von elektronischen Beweisen, um erfolgreiche Ermittlungen durchführen zu können. Gleichwohl wollen wir auch auf die negativen Aspekte hinweisen, dies könnte auch eine Schwächung der Verschlüsselung für Europas digitale Souveränität beinhalten und eine solche Maßnahme kennt man überwiegend aus autoritären Regimen. Der VDA fordert die Politik auf, jede Maßnahme zu unterlassen, die die Verschlüsselung schwächen könnte. Wir lehnen jegliche technischen Lösungen wie Backdoors strikt ab, da ihre reine Existenz die Verschlüsselung in der EU schwächen würde.

In diesem Zusammenhang ist auch zu berücksichtigen, dass die sektorspezifische Regulierung, beispielsweise im Typgenehmigungsverfahren für Fahrzeughersteller, die Ende-zu-Ende-Verschlüsselung als immanent für die Ableitung eines zusammenhängenden und kohärenten

Ansatzes für die Cybersicherheit von Produkten und Dienstleistungen betrachtet. Die Implementierung von legalen Abhörmaßnahmen birgt das nicht zu leugnende Risiko, dass die damit verbundenen Möglichkeiten nicht nur autorisierten Nutzern oder Einrichtungen offenstehen, sondern auch Angreifern, die diese aktiv ausnutzen werden. Die bisherigen Erfahrungen bei der Untersuchung der Fähigkeit von Behörden, gesetzlich geforderte Sollbruchstellen in der Informationssicherheit adäquat abzusichern, im Gegensatz zu der Fähigkeit böswilliger Angreifer, diese auszunutzen, zeigen regelmäßig ein Missverhältnis von Kompetenzen und Möglichkeiten zu Lasten der Behörden.

Liste wesentlicher und wichtiger Einrichtungen (Anhang I und II) i.V.m. den in Artikel 2 Nr. 2 vorgesehenen Ausnahmen für Kleinstunternehmen

Der Anwendungsbereich der NIS-2-Richtlinie wird im Vergleich zu ihrer Vorgängerrichtlinie (Richtlinie EU 2016/1148) breiter gefasst sein. Nur die Kleinstunternehmen und Kleinunternehmen sind von der Richtlinie ausgenommen. Die Mitgliedstaaten erstellen hierzu eine Liste der Kleinst- und Kleinunternehmen, die jedoch unter diese Richtlinie fallen werden.

VDA-Position: Um die Cybersicherheit in Europa ganzheitlich zu stärken, erscheint es gerechtfertigt, den Anwendungsbereich der Richtlinie erheblich zu erweitern, insbesondere angesichts der zunehmenden Cyberangriffe. Wir begrüßen die Ausnahmen für Kleinst- und Kleinunternehmen, da diese oft nicht über die erforderlichen finanziellen Mittel verfügen, um die in der NIS-2-Richtlinie festgelegten und zum Teil weitreichenden Verpflichtungen zu erfüllen. Wir fordern daher, dass alle KMU gemäß der Empfehlung 2003/361/EG (Artikel 2) der Kommission vom Anwendungsbereich der Richtlinie auszunehmen sind. Dies bedeutet, dass alle Unternehmen die als "wichtig" eingestuften Branchen tätig sind und unter 250 Mitarbeitern beschäftigen vom Anwendungsbereich der Richtlinie ausgenommen werden. Die zuständigen nationalen Behörden sollten jedoch Kleinst- und Kleinunternehmen in die Lage versetzen, ihre Cybersicherheitskapazitäten zu verbessern, da solche Einrichtungen häufig das Ziel von Cyberkriminellen sind.

Eine klare Definition des "Unternehmenstyps" die im Anhang I und II erwähnt werden, wäre wünschenswert. Insbesondere ist der Begriff "Cloud Computing Service Provider" in Anhang I Nr. 8 relativ weit gefasst und ungenau. Die aktuelle Formulierung umfasst beispielsweise nicht nur die Anbieter von reinen Speicher- und Rechenkapazitäten, sondern auch Softwareanbieter, die in Verbindung mit ihren virtuell nutzbaren Softwareprodukten Speicherplatz in einer Cloud anbieten. Aufgrund der weiteren Virtualisierung der Informationstechnologie könnte die sehr weit gefasste Definition dazu führen, dass sukzessive mehr Dienstleistungen in diese Kategorie fallen. Fast jeder Dienst verwendet Hosting als Teildienst. Um dies zu vermeiden, sollte die NIS-Richtlinie zwischen "digitalen Dienstleistern" einerseits und Nutzern wie "Unternehmen" oder "Betreibern wesentlicher Dienstleistungen" andererseits unterscheiden. Es sollte klargestellt werden, dass der Adressat der Vorschriften über Cloud Computing nicht alle Anbieter von Cloud-basierten Softwareprodukten sein sollten, sondern nur die Anbieter, deren Dienste wesentliche Versorgungsdienste ermöglichen. Unternehmen, die daher einen "digitalen Dienst" nutzen, um ihre Software as a Service (SaaS) anzubieten, ohne dass der Schwerpunkt ihres eigenen SaaS auf der Bereitstellung von Cloud-Kapazität für die Nutzer liegt - die daher "ein Glied weiter unten" in der "Kette" der Anbieter sind - sollten ausdrücklich vom Anwendungsbereich ausgeschlossen werden. Dies gilt umso mehr, als "Cloud Computing Service Provider" - anders als in NIS-RL 1.0 - nun unter "wesentliche Einheiten" fallen und somit weitreichenden Verpflichtungen unterliegen.

Fast das gleiche gilt für den Begriff "Anbieter von Online-Marktplätzen" in Anhang II Nr. 6. Im Gegensatz zu den "Cloud Computing Service Providern" werden erstere nicht als "Essential Entities", sondern als "Wichtige Einrichtungen" bewertet. Dennoch ist das Problem bei der Klassifizierung vergleichbar: Es gibt auch keine explizite Unterscheidung zwischen Anbietern, deren Dienstleistung in erster Linie ein Online-Marktplatz ist, und solchen Anbietern, die einen solchen Dienst lediglich als Unterangebot für einen anderen Dienst anbieten.

Koordinierte Offenlegung von Schwachstellen und europäisches Schwachstellenregister (Artikel 6)

Die Europäische Kommission strebt eine EU-weite Institutionalisierung der koordinierten Offenlegung von Anfälligkeiten an. Dazu soll ein Computer Security Incident Response Team (CSIRT) in jedem Mitgliedstaat die Koordinierung und Offenlegung von Schwachstellen sicherstellen. Das benannte CSIRT fungiert als vertrauenswürdiger Vermittler und erleichtert die Interaktion zwischen der meldenden Stelle und den Herstellern. Darüber hinaus entwickelt und unterhält die European Union Agency for Cybersecurity (ENISA) ein europäisches Schwachstellenregister, um Schwachstellen bei IT- oder Kommunikationsprodukten oder Diensten offenzulegen. Dazu soll ein Register geschaffen werden und allen interessierten Parteien Zugang zu den Informationen über die enthaltenen Schwachstellen zu gewähren.

VDA-Position: Der VDA begrüßt das Ansinnen zu mehr Sicherheit von Produkten und Dienstleistungen. Die Europäische Union sollte hier jedoch das koordinierte Offenlegen von Sicherheitslücken, beispielsweise auf der Grundlage internationaler Standards wie ISO/IEC 29147, in Betracht ziehen. Je nach Schweregrad der Sicherheitslücke (bewertet nach branchenweit anerkannten Kriterien und Standards wie ISO/IEC 29147 oder dem CVE-Framework) sollten bestimmte Zeitintervalle für die Bereitstellung von Patches oder Updates in die entsprechende Regelung aufgenommen werden. Die Verwendung von vagen Rechtsbegriffen wie "ausreichende Zeit" sollte aufgrund der damit verbundenen rechtlichen Risiken vermieden werden.
Bei der Offenlegung von Schwachstellen muss ENISA 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 Hacker die offengelegten Schwachstellen ausnutzen und zum Nachteil der Cybersicherheit in Europa führen. Daher sollte ein Zeitrahmen festgelegt werden, wie schnell ENISA den Hersteller benachrichtigen muss und wie lange der Hersteller die Anforderungen überprüfen, darauf reagieren und bei Bedarf eine Fehlerbehebung durchführen muss.
Die Meldung von Sicherheitslücken darf keine Einbahnstraße sein. Die zuständigen Behörden müssen verpflichtet werden, das Wissen über Schwachstellen ebenso zu teilen und in das Register einzupflegen.

Risikomanagement und Meldungen im Bereich Cybersicherheit (Artikel 17)

Die Mitgliedsstaaten sollen sicherstellen, dass die Leitungsorgane wesentlicher und wichtiger Einrichtungen die Cybersicherheitsrisikomanagementmaßnahmen erfüllen und deren Umsetzung überwachen. Darüber hinaus müssen die Mitglieder des Leitungsorgans spezifische Schulungen absolvieren, um ausreichende Kenntnisse und Fähigkeiten zu erwerben, um Cybersicherheitsrisiken und Managementpraktiken und ihre Auswirkungen auf die Geschäftstätigkeit des Unternehmens zu erfassen und zu bewerten.

VDA-Position: Wir halten es jedoch für äußerst wichtig, dass die Europäische Kommission anerkennt, dass Mitglieder von Leitungsorganen wesentlicher Einrichtungen und wichtiger Einrichtungen über IT-Sicherheitspersonal verfügen, das über die erforderlichen Qualifikationen verfügt, um die Cybersicherheitsstrategie eines Unternehmens ständig weiterzuentwickeln und umzusetzen. Folglich ist fraglich, ob tatsächlich Mitglieder von Leitungsorganen eine entsprechende Schulung absolvieren müssen oder ob Berichte von CISOs oder IT-Sicherheitspersonal nicht gleichermaßen ausreichen, um Mitgliedern von Leitungsorganen ausführliche Informationen zur Verfügung zu stellen.
Zumindest sollte bei der Prämisse einer unmittelbaren persönlichen Verantwortung des Managements für die Nichteinhaltung von Informationssicherheitsanforderungen berücksichtigt werden, dass die verschiedenen Mitgliedsstaaten der Europäischen Union unterschiedliche rechtliche Rahmenbedingungen für die persönliche Haftung geschaffen haben. Unter diesem Gesichtspunkt wäre zunächst eine diesbezügliche Harmonisierung im Gemeinschaftsrecht notwendig und ratsam. Darüber hinaus ist zu berücksichtigen, dass derartige Haftungsregeln

außerhalb der Europäischen Union noch nicht existieren und europäische Unternehmen daher auf globaler Ebene einen erheblichen Wettbewerbsnachteil erfahren könnten.

Wenn die Europäische Kommission jedoch eine obligatorische Weiterbildung zur IT-Sicherheit für Mitglieder von Leitungsorganen für erforderlich hält, sollte sie rasch Informationen darüber veröffentlichen, was "ausreichende Kenntnisse und Fähigkeiten" ausmacht. Darüber hinaus sollten die Empfehlungen in der gesamten EU übereinstimmen, um sicherzustellen, dass die Mitglieder der Leitungsorgane nicht mit unterschiedlichen Anforderungen im Binnenmarkt konfrontiert werden.
Der VDA fordert hierzu eine klare Definition.

Maßnahmen zum Risikomanagement im Bereich der Cybersicherheit (Artikel 18)

Wesentliche und wichtige Stellen müssen demnach einem dargestellten Risiko angemessen reagieren und das Sicherheitsniveau der Netz- und Informationssysteme gewährleisten. Dazu zählt mindestens (a) Risikoanalyse- und Sicherheitspolitiken für Informationssysteme; b) Umgang mit Vorfällen (Prävention, Erkennung und Reaktion); c) Geschäftskontinuität und Krisenmanagement; d) Die Sicherheit der Lieferkette, einschließlich sicherheitsbezogener Aspekte in Bezug auf die Beziehungen zwischen jedem Unternehmen und seinen Lieferanten oder Dienstleistern wie Anbietern von Datenspeicherungs- und -verarbeitungsdiensten oder verwalteten Sicherheitsdiensten; e) Sicherheit bei der Erfassung, Entwicklung und Wartung von Netzwerk- und Informationssystemen, einschließlich der Behandlung und Offenlegung von Schwachstellen; f) Strategien und Verfahren (Tests und Audits) zur Bewertung der Wirksamkeit von Maßnahmen zum Risikomanagement im Bereich der Cybersicherheit; und (g) die Verwendung von Kryptographie und Verschlüsselung. Die EU-Kommission kann Durchführungsrechtsakte erlassen, um die technischen und methodischen Spezifikationen dieser Elemente festzulegen. Die Kommission kann Durchführungsrechtsakte erlassen, um die technischen und methodischen Spezifikationen der oben genannten Elemente festzulegen (Absatz 5). Die Kommission ist berechtigt, delegierte Rechtsakte zu erlassen, um neuen Cyberbedrohungen, technologischen Entwicklungen oder sektoralen Besonderheiten Rechnung zu tragen (Ziffer 6).

VDA-Position: Der VDA fordert die Europäische Kommission, das Europäische Parlament und die Mitgliedstaaten auf, Maßnahmen zum Risikomanagement im Bereich von Netz- und Informationssystemen einzuführen, die ein hohes Maß für wesentliche und wichtige Stellen bietet.
Eine Rechtssicherheit für die Unternehmen zu schaffen, muss hier im Vordergrund stehen. Ein Verweis auf den "Stand der Technik" ist wenig hilfreich, zumal dies nach einem Vorfall genügend Raum für Gutachter lässt, die zu dem Schluss gelangen könnten, dass nicht alle potenziellen State-of-the-Art-Fähigkeiten angewendet wurden.
Im Hinblick auf die spezifischen Anforderungen an das Cybersecurity-Risikomanagement sollte die Europäische Kommission auch erwägen, für die operative Umsetzung der in Artikel 18 genannten Anforderungen auf branchenrelevante Standards (z. B. für Fahrzeughersteller: TISAX, ISO/SAE 21434, etc.) zu verweisen. Damit eröffnet die Kommission sowohl wesentlichen als auch wichtigen Einrichtungen die Möglichkeit, bereits bestehende Prozesse, Strukturen und Technologien im Kontext des Informationssicherheits-Risikomanagements in das Anforderungsmodell nach Artikel 18 zu integrieren und so unverhältnismäßige neue Aufwände für die Gestaltung und Implementierung neuer Prozesse und Strukturen zu vermeiden.

Meldepflichten (Artikel 20)

Wesentliche Stellen müssen Vorfälle unverzüglich beziehungsweise innerhalb von 24 Stunden nach Bekanntwerden den zuständigen Behörden oder CSIRT gemeldet werden. Darüber hinaus müssen Unternehmen spätestens einen Monat nach der Meldung von Vorfällen einen Abschlussbericht gefertigt haben. Unternehmen müssen sowohl (a) Vorfälle mit erheblichen Auswirkungen auf die Bereitstellung ihrer Dienste melden, als auch b) jede signifikante Cyberbedrohung, die diese Unternehmen identifizieren, die möglicherweise zu einem signifikanten Vorfall geführt haben könnten. Darüber hinaus müssen die Unternehmen potenziell betroffene Empfänger benachrichtigen. Unternehmen müssen nur erhebliche Vorfälle melden, d. h. solche, die erhebliche Betriebsstörungen oder finanzielle Verluste für das betreffende Unternehmen verursacht haben.

VDA-Position: In Deutschland müssen Betreiber kritische Infrastrukturen Cybersicherheitsvorfälle seit Inkrafttreten des ersten IT-Sicherheitsgesetzes im Jahr 2016 an die zuständigen nationalen Behörden, das Bundesamt für Sicherheit in der Informationstechnik (BSI), melden.

Die besondere Herausforderung im Kontext der Analyse von Cybersicherheits-Bedrohungen und der Ableitung von handlungsorientierten Erkenntnissen besteht darin, dass aufgrund der Breite und Vielfalt der dabei gewonnenen Informationen nur bestimmte Angriffsvektoren und Bedrohungen für bestimmte Einrichtungen über alle Meldeentitäten hinweg bedeutsam werden (insbesondere im Hinblick auf die in der Richtlinie definierten wichtigen Einrichtungen). Die systematische Aufbereitung der in ein zentrales Meldesystem eingespeisten Informationen und die zielgruppenspezifische Verteilung der daraus gewonnenen Erkenntnisse zum Zwecke der Abwehr potenzieller Bedrohungen ist daher ein wesentliches Kernelement eines jeden Melde- und Informationsprozesses. Bei der Einrichtung eines solchen Prozesses auf europäischer Ebene sollte in diesem Zusammenhang sichergestellt werden, dass die angeschlossenen Stellen aus den Rückmeldungen der zentralen Stellen (ENISA o.ä.) sektorspezifische, handlungsorientierte Erkenntnisse und Empfehlungen erhalten.

Wesentliche und wichtige Unternehmen profitieren nur dann von einer Meldepflicht für Bedrohungen, wenn es eine Institution – möglicherweise die ENISA – gibt, die:

- systematisch die Bedrohungen klassifiziert;
- organisiert die automatische Verteilung der Bedrohungsinformationen an die teilnehmenden Parteien;
- analysiert strategische Informationen zur Bedrohungslage;

Ferner bedarfs er einer genauen Definition des Begriffs "erheblicher Vorfall", da der derzeitige Gesetzestext viel Raum für Interpretation zulässt. Unternehmen benötigen ein hohes Maß an Rechtssicherheit, zumal wesentliche und wichtige Unternehmen, die ihren Berichtspflichten nicht nachkommen, mit einer erheblichen Geldbuße belegt werden müssen.

Allgemeine Bedingungen für die Verhängung von Geldbußen gegen wesentliche und wichtige Stellen (Artikel 31)

Die Mitgliedstaaten können Geldbußen wegen Verstößen bei mangelnden Maßnahmen zum Risikomanagement im Bereich der Cybersicherheit (Artikel 18) und bei fehlenden Meldepflichten (Artikel 20) verhängen. Die Verwaltungsstrafen belaufen sich auf höchstens 10.000.000 Euro oder bis zu zwei Prozent des weltweiten Jahresumsatzes.

VDA-Position: Um sicherzustellen, dass alle Unternehmen die in Artikel 18 vorgesehenen Maßnahmen zur Minderung des Cybersicherheitsrisikos umsetzen und ihren Meldepflichten nach Artikel 20 nachkommen, erscheint die Einführung von Bußgeldern plausibel. Der VDA fordert jedoch eine deutliche Senkung der Verwaltungsstrafen. Denn anders als beim Datenschutz wird hier kein Grundrecht (Recht auf informationelle Selbstbestimmung) verletzt. Auch die datenschutzrechtlichen Erwägungen, die dazu geführt haben, dass Bußgelder auf der Grundlage von Konzernverkäufen berechnet wurden, passen hier nicht. Die Höchsthöhe der Verwaltungsstrafen sollte angemessen und nicht höher als max. zwei Millionen Euro sein, ohne dass auf den Jahresumsatz Bezug genommen wird. Ein solches Niveau würde ein akzeptables Gleichgewicht zwischen der Absicht, die Unternehmen zu bestrafen, die gegen die Anforderungen der Artikel 18 und 20 verstoßen, und den Anforderungen der deutschen Automobilindustrie an Verwaltungsstrafen, die nicht übermäßig sind finden.

Herausgeber	Verband der Automobilindustrie e.V. (VDA) Behrenstraße 35, 10117 Berlin www.vda.de
Copyright	Verband der Automobilindustrie e.V. (VDA)
Stand	März 2021

VDA | Verband der Automobilindustrie