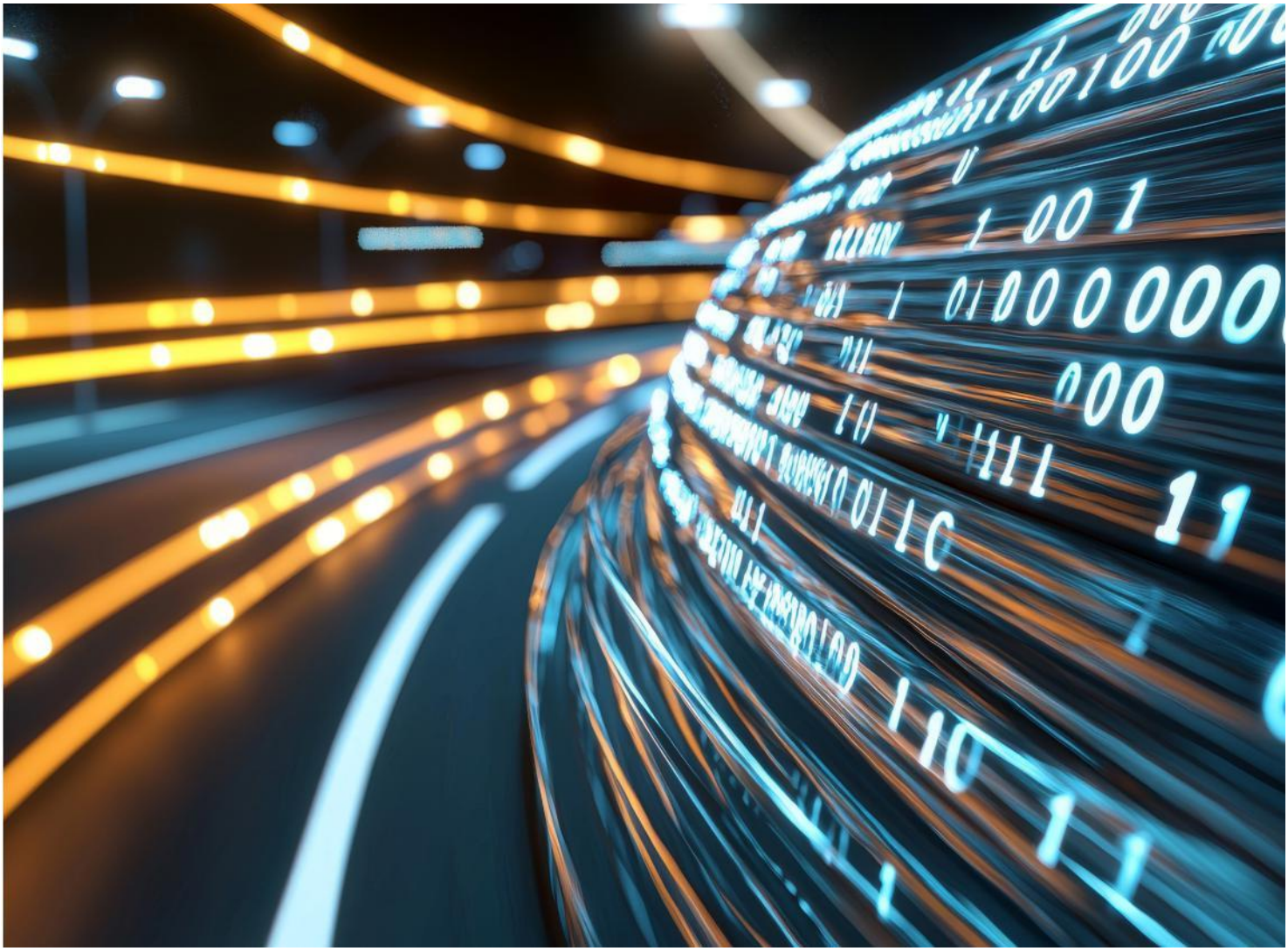
VDA Verband der Automobilindustrie

Empfehlung

Zum aktuellen Referentenentwurf der NIS-2-Richtlinie

Impulse für eine praxistaugliche Umsetzung



1. Einführung

Der Verband der Automobilindustrie (VDA) nutzt die Möglichkeit, zum aktuellen Referentenentwurf des Bundesministeriums des Innern für ein Gesetz zur Umsetzung der NIS-2 -Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz – NIS2UmsuCG) in der Fassung vom 23.06 2025 Stellung nehmen zu können. Wir begrüßen ausdrücklich, dass mit der Umsetzung der NIS-2-Richtlinie der bestehende Ordnungsrahmen, der durch das Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) von 2015 sowie das IT-Sicherheits-gesetz 2.0 von 2021 geschaffen wurde, weiterentwickelt und an die gestiegenen Anforderungen angepasst wird.
Mit der Umsetzung der NIS-2-Richtlinie werden insbesondere neue Verpflichtungen für Unternehmen eingeführt, zugleich enthält der Entwurf erstmalig verbindliche Regelungen für die Bundesverwaltung. Aus Sicht des VDA sind dabei ein ganzheitlicher Ansatz zur Erhöhung des Schutzes vor digitalen und analogen Bedrohungen, eine verstärkte Kooperation zwischen Staat und Wirtschaft sowie die Einführung effizienter Prozesse und risikoadäquater Anforderungen von zentraler Bedeutung.
Angesichts der weiter zunehmenden Cybersicherheitsvorfälle, die sich auch immer häufiger gegen Städte, Landkreise und öffentliche Einrichtungen richten, ist eine widerstandsfähige öffentliche Verwaltung von großer Bedeutung – für Bürger, Wirtschaft und Industrie gleichermaßen. Auch für die deutsche Automobilindustrie ist die Sicherheit kritischer Infrastrukturen essenziell, da Lieferketten, Produktion und Entwicklung in hohem Maße von funktionierenden Verwaltungs- und Versorgungsstrukturen abhängig sind.
Darüber hinaus halten wir es für notwendig, für die Durchführung wirksamer Penetrationstests auch sog. ethische Hacker einzubeziehen. In der nationalen Umsetzung der NIS-2 sollte daher eine ausdrückliche Klarstellung aufgenommen werden, um ethische Hacker im Rahmen legaler Sicherheitsprüfungen von einer Strafbarkeit nach § 202a StGB auszunehmen. Dies würde für Rechtssicherheit sorgen und Unternehmen ermöglichen, Schwachstellen frühzeitig und effizient zu identifizieren und zu schließen.
In der Anlage 2 des Referentenentwurfs wird unter Nummer 5.5 die Herstellung von Kraftwagen und Kraftwagenteilen namentlich benannt. Damit ist eindeutig festgelegt, dass auch die deutsche Automobilindustrie als „wichtige Einrichtung“ im Sinne des Gesetzes betroffen ist.

2. Zusammenfassung der Empfehlungen

Der Verband der Automobilindustrie (VDA) begrüßt grundsätzlich den aktuellen Referentenentwurf des Bundesministeriums des Innern zur Umsetzung der NIS-2-Richtlinie vom 23. Juni 2025. Die Weiterentwicklung des bestehenden Ordnungsrahmens hin zu höheren Anforderungen an die Informationssicherheit wird als notwendig erachtet. Dabei betont der VDA die Bedeutung eines ganzheitlichen Ansatzes, der sowohl digitale als auch analoge Bedrohungen berücksichtigt, sowie die Wichtigkeit einer engen Kooperation zwischen Staat und Wirtschaft. Problematisch ist, dass es aufgrund der föderalen Strukturen keinen ganzheitlichen flächendeckenden Ansatz gibt, der digitale und analoge Bedrohungen berücksichtigt. Langfristig wäre es deshalb zum effektiven Schutz sensibler Daten zwingend erforderlich, die Anforderungen an die Informationssicherheit auch auf Länder- und Kommunalebene zu erweitern.

Zudem plädiert der VDA dafür, sogenannte ethische Hacker explizit in die Durchführung von Sicherheitsprüfungen einzubeziehen. Um Rechtssicherheit zu schaffen, sollte eine gesetzliche Klarstellung erfolgen, die ethische Hacker im Rahmen legaler Penetrationstests von strafrechtlichen Konsequenzen freistellt.

Für die Automobilindustrie besonders relevant ist, dass in Anlage 2 des Referentenentwurfs die Herstellung von Kraftwagen und Kraftwagenteilen als „wichtige Einrichtung“ festgelegt ist, wodurch die Branche direkt betroffen ist.

Der Entwurf führt die neuen Kategorien „besonders wichtige Einrichtungen“ und „wichtige Einrichtungen“ ein und erweitert somit den bisherigen Anwendungsbereich. Der Katalog der Mindestsicherheitsanforderungen aus Artikel 21 der NIS-2-Richtlinie wird in das BSI-Gesetz integriert, wobei die Anforderungen differenziert ausgestaltet werden sollen. Das bisherige einstufige Meldeverfahren wird durch ein dreistufiges Meldesystem ersetzt. Positiv bewertet der VDA, dass der bürokratische Aufwand im Rahmen des mitgliedstaatlichen Spielraums möglichst geringgehalten werden soll. Gleichzeitig wird das Instrumentarium des Bundesamts für Sicherheit in der Informationstechnik (BSI) im Bereich Aufsichts- und Durchsetzungsmaßnahmen erweitert. Für die Wirtschaft ergeben sich erhebliche zusätzliche Aufwände von mehreren Milliarden Euro jährlich, insbesondere für die Einführung digitaler Prozesse. Der VDA fordert daher praxistaugliche, effiziente und unbürokratische Lösungen.

Im Rahmen der Registrierungspflichten müssen sich betroffene Unternehmen innerhalb von drei Monaten registrieren. Wichtig ist aus Sicht des VDA, dass relevante Informationen von staatlichen Stellen automatisiert bereitgestellt werden, um die Betroffenheit frühzeitig zu klären. Um Bürokratie zu vermeiden, sollte für Unternehmen mit Niederlassungen in mehreren EU-Staaten eine konsolidierte Bescheinigung ausreichend sein. Gleiches gilt für Unternehmensverbünde, die eine gemeinsame Registrierung vornehmen sollten, da sie häufig gemeinsame Infrastrukturen nutzen. Kritisch sieht der VDA die vorgesehene Verkürzung der Frist für Änderungsmeldungen auf lediglich zwei Wochen, was eine deutliche Verschärfung gegenüber der NIS-2-Richtlinie darstellt und dringend korrigiert werden sollte.

Bei den Meldepflichten fordert der VDA den Aufbau eines vollständig digitalen, effizienten Meldeportals durch das BSI in Zusammenarbeit mit der Europäischen Kommission und ENISA. Um insbesondere mittelständische Unternehmen zu entlasten, sollte die Pflicht zur Zwischenmeldung in der Praxis entfallen. Das BSI sollte stattdessen sein Beratungsangebot ausbauen. Der VDA unterstützt die Nutzung des im Rahmen des Onlinezugangsgesetzes entwickelten Organisationskontos als zentrale Schnittstelle zwischen Staat und Wirtschaft. Meldungen aus Konzernverbünden sollten gebündelt erfolgen können, um den Verwaltungsaufwand zu verringern. Auch die Möglichkeit, Meldungen in englischer Sprache einzureichen, wird als sinnvoll angesehen. Grundsätzlich fordert der VDA eine enge nationale und internationale Koordinierung, um Doppelmeldungen zu vermeiden.

Besonders wichtig ist dem VDA der Schutz sensibler Unternehmens- und Kundendaten im Rahmen der Meldepflichten. Gerade kleine und mittlere Unternehmen benötigen praxisnahe Lösungen und eine zentrale Anlaufstelle, idealerweise beim BSI, um das sogenannte Once-Only-Prinzip umzusetzen. Zudem sollte sichergestellt werden, dass eine einmalige Meldung auf europäischer Ebene für multinationale Unternehmen ausreicht. Insgesamt sieht der VDA dringenden Verbesserungsbedarf bei der praktischen Ausgestaltung der Meldepflichten, insbesondere zur Vermeidung von Doppelarbeit und ineffizienten Prozessen.

Ein weiterer kritischer Punkt ist die erweiterte persönliche Haftung der Geschäftsleitung für das Cyber-Risikomanagement. Hier fordert der VDA die Möglichkeit einer wirksamen Delegation der Pflichten sowie die Prüfung ergänzender Safe-Harbor-Regelungen, um Rechtssicherheit zu schaffen und insbesondere mittelständische Unternehmen vor übermäßigen Risikenzu schützen.

Die Kostenschätzungen des Referentenentwurfs hält der VDA für unzureichend begründet, insbesondere in Bezug auf KRITIS-Unternehmen. Wir fordern deshalb verbindliche Umsetzungshilfen und transparente Kalkulationen.

Zudem gibt es aus Sicht der Unternehmen weiterhin Unsicherheiten darüber, ob sie tatsächlich als betroffene Einrichtung gelten, mit Ausnahme der klar benannten Automobilbranche. Gerade bei Bereichen wie digitaler Infrastruktur oder IT-Dienstleistungen herrscht Klärungsbedarf. Auch die Möglichkeit zu Sicherheitsüberprüfungen für Beschäftigte in sicherheitskritischen Bereichen sollte geschaffen werden. Dafür müssten gegebenenfalls Anpassungen im Datenschutzrecht erfolgen, wobei gleichzeitig ausreichende Ressourcen für solche Prüfungen durch die öffentliche Hand bereitgestellt werden müssten.

Die Einführung des „CISO Bund“ für die Bundesverwaltung wird begrüßt. Für Unternehmen sollte die Möglichkeit bestehen, ebenfalls eine vergleichbare Funktion zu benennen, wobei eine flexible Ausgestaltung gefordert wird, um der Unternehmensvielfalt gerecht zu werden. Positiv bewertet wird hingegen die Streichung der Kategorie „Unternehmen im besonderen öffentlichen Interesse“, was zu mehr Transparenz beiträgt. Zudem sollte der Gesetzgeber Schwellenwerte für kritische Anlagen klar und verbindlich festlegen, um den Unternehmen verlässliche Orientierung zu bieten.

Im Einzelnen:

3. Registrierungspflichten

Im Rahmen der Umsetzung der NIS-2-Richtlinie wird von Unternehmen, die als „besonders wichtige“ oder „wichtige Einrichtungen“ eingestuft sind, erwartet, dass sie sich spätestens innerhalb von drei Monaten nach Feststellung ihrer Betroffenheit registrieren (§33, §34 des aktuellen Referentenentwurfs vom 23. Juni 2025). Die Registrierung soll über ein zentrales Internetportal erfolgen. Eine entscheidende Voraussetzung für eine praxistaugliche Umsetzung ist die automatisierte Bereitstellung relevanter Informationen durch die zuständigen staatlichen Stellen, damit Unternehmen frühzeitig und verlässlich Kenntnis über ihre Betroffenheit erhalten.
Zur Vermeidung unnötiger Bürokratie sollten Unternehmen mit Niederlassungen in mehreren EU-Mitgliedstaaten die Möglichkeit erhalten, eine konsolidierte Bescheinigung ihrer jeweiligen nationalen Behörde vorzulegen. Diese Bescheinigung sollte die europaweite Unternehmensstruktur abbilden und von den zuständigen Behörden anderer Mitgliedstaaten anerkannt werden. Ein solches Verfahren wäre geeignet, Doppelarbeit zu vermeiden und den Verwaltungsaufwand für international tätige Unternehmen erheblich zu reduzieren.
Für Unternehmen in einem Konzernverbund sollte eine gemeinsame Registrierung aller verbundenen Unternehmen ermöglicht werden. Da verbundene Unternehmen regelmäßig gemeinsame Dienste, Infrastrukturen und Prozesse nutzen, würde eine konsolidierte Registrierung den Aufwand für alle Beteiligten – insbesondere für die betroffenen Unternehmen und das BSI – deutlich reduzieren. Nachteile einer gemeinsamen Registrierung sind aus Sicht des VDA nicht ersichtlich, sofern die betroffenen Unternehmen eindeutig benannt werden.
Mit dem Inkrafttreten und der parallelen Umsetzung der NIS-2-Richtlinie sowie der CER-Richtlinie für KRITIS-Betreiber wird eine Vielzahl weiterer Unternehmen zusätzlich zu den bisherigen Anforderungen des IT-Sicherheitsgesetzes 2.0 registrierungspflichtig. Diese Pflichten sollten effizient, digital und an den praktischen Bedürfnissen der Wirtschaft ausgerichtet gestaltet werden. Der Zugang staatlicher Stellen zu Unternehmensdaten sollte ausschließlich nach dem Need-to-know-Prinzip erfolgen.

Die Bündelung aller relevanten Informationen zu einem Cybervorfall an einer zentralen Stelle würde prozessuale Vorteile bieten, sofern dabei angemessene Sicherheitsstandards für die Informationsübertragung und -speicherung gewährleistet sind.
Angesichts der großen Zahl betroffener Unternehmen sollte geprüft werden, inwieweit Unternehmens- und Branchenverbände aktiv in den Prozess eingebunden werden können, um ihre Mitglieder bei der Registrierung zu unterstützen.
Besonders kritisch sieht der VDA die im Referentenentwurf vorgesehene Verkürzung der Änderungsfrist für Registrierungsdaten auf lediglich zwei Wochen (§34). Diese Frist liegt deutlich unter der von der NIS-2-Richtlinie vorgesehenen Drei-Monats-Frist und stellt eine erhebliche Belastung insbesondere für größere Unternehmensstrukturen dar.
Eine solche nationale Verschärfung ist aus Sicht des VDA nicht sachgerecht und sollte dringend zurückgenommen werden, um den Unternehmen einen realistischen Zeitraum für die Erfüllung ihrer Meldepflichten einzuräumen.

4. Meldepflichten

Vor dem Hintergrund der erheblichen Ausweitung der Meldepflichten, die im NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG) vorgesehen sind – von einer Meldung pro Vorfall nach IT-Sicherheitsgesetz 2.0 auf bis zu fünf Meldungen, sowie von tatsächlichen zu auch potenziellen Vorfällen – ist es von entscheidender Bedeutung, dass das Bundesamt für Sicherheit in der Informationstechnik (BSI) in enger Zusammenarbeit mit der Europäischen Kommission, der Europäischen Agentur für Cybersicherheit (ENISA) und unter Einbeziehung des Bundesamts für Bevölkerungsschutz und Katastrophenhilfe (BBK) ein effizientes, vollständig digitalisiertes und interoperables Meldeportal errichtet.
Dieses Portal muss gewährleisten, dass die ohnehin knappen Meldefristen nicht zusätzlich durch Mehrfachmeldungen, uneinheitliche Formate oder redundante Informationsabfragen verkürzt werden. Um den erheblichen Erfüllungsaufwand für die Unternehmen zu begrenzen, sollte das BSI in der Praxis von der Pflicht zur Zwischenmeldung gemäß §32 Abs. 1 Nr. 3 des Referentenentwurfs weitgehend absehen. Insbesondere mittelständische Unternehmen sind bei der Bewältigung eines schwerwiegenden Sicherheitsvorfalls vollständig mit der operativen Reaktion auf den Vorfall gebunden. Eine verpflichtende Zwischenmeldung bindet hierfür dringend benötigte personelle und finanzielle Ressourcen. Um eine übermäßige Belastung der Unternehmen zu vermeiden, sollten stattdessen das Beratungsangebot des BSI gemäß §36 Abs. 1 gestärkt und sämtliche relevanten Sicherheitsbehörden aktiv in den Unterstützungsprozess eingebunden werden.
Der VDA unterstützt nachdrücklich die Nutzung des im Rahmen des Onlinezugangsgesetzes entwickelten Organisationskontos als zentrale Kommunikationsschnittstelle zwischen Wirtschaft und Verwaltung. Die konsequente Nutzung dieser Infrastruktur würde den bürokratischen Aufwand erheblich reduzieren, redundante Meldestrukturen vermeiden und die Umsetzungskosten auf Unternehmensseite deutlich senken. Gleichzeitig würde die Nutzung des Organisationskontos das Once-Only-Prinzip konkret umsetzen und damit den nationalen Digitalisierungszielen gerecht werden.
Zur weiteren Reduzierung der Komplexität des Meldeverfahrens sollte Unternehmen innerhalb eines Konzernverbunds die Möglichkeit eingeräumt werden, Meldungen zu einem einheitlichen Sachverhalt in einer konsolidierten, gemeinsamen Meldung zusammenzufassen. Diese Bündelung führt weder zu einem Informationsverlust noch zu einem Mehraufwand, sondern erhöht die Transparenz, Effizienz und Geschwindigkeit sowohl auf Seiten der meldenden Unternehmen als auch der zuständigen Behörden.

Für international tätige Unternehmen, deren IT-Sicherheitsstrukturen in der Regel auf Englisch arbeiten, sollte darüber hinaus die Möglichkeit geschaffen werden, Meldungen an das BSI auch in englischer Sprache abzugeben. Dies würde nicht nur die Bearbeitung auf Seiten des BSI erleichtern, sondern auch die Zusammenarbeit mit internationalen Partnerbehörden und Organisationen, insbesondere ENISA, verbessern. Die im Referentenentwurf vorgesehenen Fristen scheinen grundsätzlich umsetzbar, bedürfen jedoch einer engen nationalen und internationalen Abstimmung, um widersprüchliche Anforderungen zu vermeiden.
Unverzichtbar ist eine klare gesetzliche Regelung zur Zusammenarbeit der beteiligten Behörden sowie eine ausdrückliche Verpflichtung zum Schutz der Unternehmens- und Kundendaten. Gerade im Kontext der Melde- und Dokumentationspflichten sensibler Informationen müssen höchste Anforderungen an den Datenschutz und die Informationssicherheit gelten.
Besonders für kleine und mittlere Unternehmen (KMU) der Automobilindustrie ist eine praxisgerechte, unbürokratische und schlanke Umsetzung der Meldepflichten essenziell, da sie oft nicht über eigene spezialisierte IT-Sicherheitsabteilungen verfügen. Es sollte daher auf Bundesebene eine zentrale Anlaufstelle für alle Meldungen geschaffen werden, die das Once-Only-Prinzip in der Praxis sicherstellt. Das BSI könnte diese Rolle übernehmen und dabei eine Koordinierungsfunktion zwischen Bund, Ländern und beteiligten Institutionen wahrnehmen. Die Bundesregierung sollte zudem sicherstellen, dass eine einmalige Meldung auf europäischer Ebene ausreichend ist, insbesondere bei länderübergreifenden Vorfällen multinational tätiger Unternehmen. Die nationale Umsetzung der NIS-2 in den einzelnen EU-Mitgliedstaaten darf nicht dazu führen, dass Unternehmen identische Vorfälle mehrfach in verschiedenen Mitgliedstaaten melden müssen. Alternativ könnte bei länderübergreifenden Vorfällen eine zentrale Meldung an ENISA als europäischer Anlaufstelle in Betracht gezogen werden.
Darüber hinaus besteht bereits auf Basis der EU-General-Safety-Regulation eine Berichtspflicht der Automobilindustrie gegenüber nationalen Behörden. Es ist sicherzustellen, dass keine doppelten Berichtspflichten für identische Sachverhalte entstehen, um unnötigen administrativen Aufwand für Unternehmen wie auch für Behörden zu vermeiden.
Der VDA fordert die Bundesregierung daher auf, den bestehenden Gestaltungsspielraum konsequent zu nutzen, um ein Meldewesen zu schaffen, das effizient, verhältnismäßig und praxistauglich ausgestaltet ist und gleichzeitig den europäischen Anforderungen gerecht wird.

5. Managerhaftung

Der aktuelle Referentenentwurf des Bundesministeriums des Innern vom 23. Juni 2025 geht an mehreren Stellen über die Vorgaben der NIS-2-Richtlinie hinaus. Dies gilt insbesondere für die persönliche Verantwortlichkeit der Geschäftsleitung für die Überwachung des Cyber-Risikomanagements in besonders wichtigen und wichtigen Einrichtungen (§38 RefE-NIS2).
Der Referentenentwurf sieht vor, dass die Verantwortung der Geschäftsleitung für die Umsetzung und Überwachung der erforderlichen Maßnahmen nicht delegierbar ist. Geschäftsleiter können demnach künftig persönlich haftbar gemacht werden – auch im Hinblick auf Regressansprüche sowie Bußgeldforderungen. Ein Verzicht auf Schadenersatzansprüche oder der Abschluss eines Vergleichs ist ausschließlich im Falle einer Insolvenz der betreffenden Einrichtung zulässig.
Dies stellt eine erhebliche Ausweitung der persönlichen Haftung dar – insbesondere für Geschäftsführerinnen und Geschäftsführer von Gesellschaften mit beschränkter Haftung (GmbHs), für die bislang rechtlich die Möglichkeit bestand, operative Aufgaben und Verantwortlichkeiten im Bereich IT-Sicherheit wirksam zu delegieren.
Der VDA sieht diese Ausgestaltung mit großer Sorge. Gerade mittelständische Unternehmen drohen dadurch unverhältnismäßigen Haftungsrisiken ausgesetzt zu werden.

Eine nationale Verschärfung über die Vorgaben der NIS-2-Richtlinie hinaus konterkariert zudem den Grundsatz der Harmonisierung innerhalb der Europäischen Union.
Der VDA fordert daher, im Gesetzgebungsverfahren klare Möglichkeiten zur wirksamen Delegation von Aufgaben vorzusehen, ergänzt um Safe-Harbor-Regelungen, um Unternehmensleitungen Rechtssicherheit zu geben, wenn sie die gesetzlichen Vorgaben nachweislich sorgfältig erfüllen. Vor diesem Hintergrund hält der VDA die Einführung einer Safe-Harbor-Regelung für zwingend erforderlich, um Rechtssicherheit für Unternehmensleitungen zu schaffen. Eine persönliche Haftung der Geschäftsleitung sollte
entfallen, wenn diese nachweislich ihre Pflichten zur Einrichtung, Überwachung und Umsetzung der notwendigen Risikomanagementmaßnahmen mit der gebotenen Sorgfalt wahrgenommen hat. Dazu gehört insbesondere die wirksame Einrichtung eines Informationssicherheitsmanagementsystems, die Bestellung fachlich geeigneter Informationssicherheitsbeauftragter sowie die regelmäßige Überprüfung der Angemessenheit der getroffenen Maßnahmen.
Eine solche Regelung würde verhindern, dass Geschäftsleitungen trotz pflichtgemäßen Handelns in eine Haftungsfalle geraten. Gleichzeitig würde sie Unternehmen einen klaren Handlungsrahmen bieten, wie sie ihren gesetzlichen Verpflichtungen gerecht werden können.
Der VDA regt daher an, diese Safe-Harbor-Regelung entweder ausdrücklich in den Gesetzestext selbst oder zumindest klarstellend in die Gesetzesbegründung aufzunehmen.
Die persönliche Haftung der Geschäftsleitung sollte sich zudem an den allgemeinen gesellschaftsrechtlichen Grundsätzen orientieren, wonach eine Haftung regelmäßig nur bei grober Pflichtverletzung in Betracht kommt. Eine sorgfältige Organisation des Informationssicherheitsmanagements und die lückenlose Dokumentation der ergriffenen Maßnahmen sollten in diesem Zusammenhang als Entlastungsnachweis dienen.
Somit würde eine ausgewogene Regelung geschaffen, die sowohl den Schutz der betroffenen Einrichtungen stärkt als auch die Handlungsfähigkeit der Unternehmensleitungen wahrt. Nur so kann verhindert werden, dass engagierte Geschäftsleitungen in eine Haftungsfalle geraten, die weder von der europäischen NIS-2-Richtlinie gefordert noch sachlich geboten ist.

6. Umsetzung der Risikomanagementmaßnahmen

In der deutschen Gesetzgebung erfolgt keine detaillierte Konkretisierung der Erwartungen an Unternehmen und Behörden hinsichtlich der in Artikel 21 der NIS-2 genannten Risikomanagementmaßnahmen. Insbesondere bleibt unklar, wie diese Maßnahmen unter Berücksichtigung von Kritikalität, Sektor, Unternehmensgröße und weiteren Einflussfaktoren anzuwenden sind. Die bisherige Aufwandsschätzung für die deutsche Wirtschaft bietet lediglich einen groben Anhaltspunkt für den Umsetzungsaufwand und stellt keine verlässliche Informationsquelle dar. So wird beispielsweise angenommen, dass KRITIS-Unternehmen keinen zusätzlichen Aufwand für die Umsetzung der NIS-2 hätten, was durch Rückmeldungen betroffener Unternehmen eindeutig widerlegt wird. Auch die Annahme, dass 17 % der Unternehmen keinen weiteren Umsetzungsbedarf hätten, ist stark zu hinterfragen. Zudem ist die Gleichsetzung des Aufwands zur Umsetzung der bisherigen NIS-Richtlinie mit dem der NIS-2-Richtlinie nicht gerechtfertigt. Lediglich die Annahme, dass große bedeutende Einrichtungen im Vergleich zu wesentlichen Einrichtungen einen um 70 % höheren Umsetzungsaufwand haben und mittlere bedeutende Einrichtungen um 35 % mehr Aufwand als wesentliche Einrichtungen benötigen, kann allein als grober Anhaltspunkt für die gesetzgeberische Erwartungshaltung betrachtet werden. Vor diesem Hintergrund ist eine Umsetzungshilfe des BSI dringend erforderlich, die konkreten Erwartungen und Maßnahmenkataloge für die betroffenen Einrichtungen definiert. Nur so können Unternehmen und Behörden in die Lage versetzt werden, die erforderlichen Maßnahmen fristgerecht und zielgerichtet umzusetzen.

Eine fundiertere Herleitung der Umsetzungskosten sowie eine praxisorientierte Handreichung des BSI zu den erwarteten Maßnahmen würden den betroffenen Unternehmen eine erhebliche Unterstützung bieten.

7. Streichung „Unternehmen im besonderen öffentlichen Interesse“

Der VDA begrüßt ausdrücklich die Entscheidung zur Streichung der Kategorie „Unternehmen im besonderen öffentlichen Interesse“ und die daraus resultierende Konzentration auf wichtige und besonders wichtige Einrichtungen, anstelle einer weiteren Differenzierung. Diese Maßnahme führt zu einer Vereinfachung und klaren Ausrichtung im Bereich der Cybersicherheitsregulierung und trägt zur Harmonisierung auf europäischer Ebene bei. Es ist erfreulich, dass Deutschland den Weg der europaweiten Standardisierung unterstützt und den Sonderweg, der durch das IT-Sicherheitsgesetz 2.0 eingeführt wurde, aufgegeben hat.

Es wäre jedoch wünschenswert, dass die Schwellenwerte für kritische Anlagen direkt im NIS2 UmsuCG festgelegt werden, anstatt auf eine nachgelagerte Rechtsverordnung zu verweisen. Durch eine direkte Festlegung im Gesetz würde Transparenz geschaffen und eine klare Orientierung für betroffene Unternehmen ermöglicht. Dies würde den Umsetzungsprozess erleichtern und eine schnellere Anpassung an die gesetzlichen Anforderungen ermöglichen.

8. Sektoren

Es ist für Unternehmen bereits jetzt schwierig, mithilfe des Anhang I und II der NIS-2 festzustellen, ob sie unter diese Regulierung fallen. Für die Automobilbranche stellt sich dies leichter dar. Allerdings kann ein Unternehmen auch mit mehreren Sektoren betroffen sein, und diese sind bei der Registrierung anzugeben.

Bei einigen Sektoren herrscht große Unsicherheit bei den betroffenen Unternehmen. Bspw. „Digitale Infrastruktur“ könnte alle deutsche Muttergesellschaften betreffen, welche ihre Rechenzentrumsdienstleistungen an ihre europäischen Tochtergesellschaften anbieten. Diese wären dann „Wesentliche Einrichtungen“.

Vom Sektor „Verwaltung von Informationstechnologie und Telekommunikation“ könnten theoretisch alle Einrichtungen betroffen sein, welche SOC-Dienstleistungen (Security Operation Center) für die europäischen Unternehmen im Konzernverbund anbieten. Dies könnte als Beispiel dazu führen, dass das indische Tochterunternehmen aufgrund seiner SOC-Dienstleistungen NIS-2-relevant wird.

Eine Klarstellung in diesen beiden Sektoren würde den deutschen Unternehmen helfen sich auf die Umsetzung als wesentliche oder wichtige Einrichtung vorzubereiten.

9. Informationssicherheitsbeauftragter (CISO)

Auf Bundesebene wird ein „CISO-Bund“ eingeführt. Im Rahmen der NIS-2 Umsetzung bietet sich die Gelegenheit, einen verantwortlichen CISO pro betroffene Einrichtung einzurichten, der bei der Registrierung auch benannt werden könnte (analog zum Datenschutz-beauftragten bei den Datenschutzbehörden).

Dabei kann der Gesetzgeber beispielsweise auf die bewährten Vorgaben der Finanzregulatorik zurückgreifen und die BAIT 4.4-4.6 (Bankaufsichtliche Anforderungen an die IT) nachbilden: „Die Geschäftsleitung hat die Funktion des Informationssicherheits-beauftragten einzurichten. Diese Funktion umfasst die Verantwortung für die Wahrnehmung aller Belange der Informationssicherheit innerhalb des Instituts und gegenüber Dritten. Sie stellt sicher, dass die in der IT-Strategie, der Informationssicherheitsleitlinie und den Informationssicherheitsrichtlinien des Instituts festgelegten Ziele und Maßnahmen hinsichtlich der Informationssicherheit sowohl intern als auch gegenüber Dritten transparent gemacht und deren Einhaltung regelmäßig sowie anlassbezogen überprüft und überwacht werden."

Dabei sollte der Vorgabe der Finanzinstitute gefolgt werden, dass die Funktion des Informationssicherheitsbeauftragten von den Bereichen getrennt wird, die für den Betrieb und die Weiterentwicklung der IT-Systeme zuständig sind. Damit wird ausgeschlossen, dass der Informationssicherheitsbeauftragte dem IT-Leiter unterstellt ist. Dies beugt Interessenkonflikten massiv vor und unterstreicht die deutlich umfangreichere Aufgabe des Informationssicherheitsbeauftragten, welche weit über die Belange der IT-Sicherheit hinausgeht.

10. Überprüfungsmöglichkeiten der Vertrauenswürdigkeit von Beschäftigten

Beschäftigte sind zweifellos das Hauptziel für Cyberangriffe. Die Wirksamkeit der technischen, organisatorischen und operativen Maßnahmen gemäß der NIS-2-Richtlinie wird beeinträchtigt, wenn nicht auch der personelle Aspekt angemessen berücksichtigt wird. Neben Schulungen für Geschäftsleitungen und Mitarbeiter gemäß § 38 Abs.3 ist es wichtig, potenzielle Risiken zu minimieren. Dies betrifft auch die Gefahr von Insider-Bedrohungen durch nicht identifizierte interne Täter, die den Wirtschaftsschutz gefährden können.

Deshalb sollten alle Unternehmen, die dem Anwendungsbereich des NIS-2-Umsetzungsgesetzes unterliegen, die Möglichkeit erhalten, Sicherheitsüberprüfungen für ihre Beschäftigten bei den entsprechenden Stellen zu beantragen. Dabei müssen die rechtlichen Voraussetzungen, insbesondere im Bundesdatenschutzgesetz (BDSG), beachtet und gegebenenfalls angepasst werden. Die Verfahren für Sicherheitsüberprüfungen sollten effizienter gestaltet und an die Bedürfnisse der Unternehmen angepasst werden. Es ist wichtig, ausreichende finanzielle und personelle Ressourcen auf staatlicher Seite bereitzustellen, um dies zu gewährleisten.

11. Fehlende Aufnahme öffentliche Verwaltung

Bislang ist die öffentliche Verwaltung der Länder und Kommunen nur unzureichend in den Anwendungsbereich einbezogen. Diese Situation erfordert dringend Verbesserungen, da die Automobilindustrie auf eine reibungslos funktionierende öffentliche Verwaltung auf allen staatlichen Ebenen angewiesen ist, die nicht durch Cyber-Sicherheitsvorfälle über einen längeren Zeitraum beeinträchtigt wird. Neben den Bundesbehörden sollten auch die Behörden der Länder und Kommunen insbesondere Genehmigungs- und Überwachungsbehörden, die sensible Daten verarbeiten und für besonders wichtige Einrichtungen essenzielle Verwaltungsdienstleistungen erbringen als „besonders wichtige Einrichtungen" definiert werden.

12. Konzernprivileg bei Digital Infrastructure Services

Im aktuellen Referentenentwurf zur Umsetzung der NIS-2-Richtlinie wird bei der Einstufung und Regulierung von Digital Infrastructure Services nicht zwischen marktbezogener Leistungserbringung und konzerninterner Bereitstellung unterschieden. Dies führt dazu, dass Unternehmen, die digitale Infrastrukturdienste ausschließlich innerhalb eines Konzernverbunds bereitstellen – etwa Rechenzentrumsleistungen, Cloud-Dienste oder Security Operations Center (SOC) – denselben regulatorischen Anforderungen unterliegen wie Anbieter, die diese Leistungen öffentlich am Markt anbieten.
Aus Sicht des VDA ist diese Gleichbehandlung nicht sachgerecht. Die Erbringung von Digital Infrastructure Services innerhalb eines Konzerns unterscheidet sich grundlegend von der marktbezogenen Bereitstellung. Sie erfolgt in einem geschlossenen, organisatorisch und technisch integrierten Umfeld, in dem zentrale Steuerung, abgestimmte Sicherheitsstandards und gemeinsame Governance-Strukturen bestehen. Die Risiken, insbesondere im Hinblick auf externe Angriffsflächen, sind in der Regel deutlich geringer.
Daher sollte bei der nationalen Umsetzung der NIS-2-Richtlinie ein sogenanntes „Konzernprivileg“ eingeführt werden. Dieses sollte vorsehen, dass Unternehmen innerhalb eines Konzerns nur dann als Betreiber digitaler Infrastrukturdienste im Sinne der NIS-2 gelten, wenn sie diese Leistungen auch gegenüber externen Dritten erbringen. Die rein konzerninterne Erbringung sollte nicht automatisch zur Anwendung der vollen Anforderungen an Risikomanagement, Meldepflichten und Aufsicht führen. Stattdessen sollte die Betroffenheit solcher Einheiten ausschließlich auf Basis ihrer Einstufung als „wichtige“ oder „besonders wichtige Einrichtung“ erfolgen und nicht aufgrund der Art der bereitgestellten Dienste.
Ein solches Konzernprivileg würde nicht nur der tatsächlichen Risikolage besser Rechnung tragen, sondern auch unnötige regulatorische Belastungen vermeiden und die Umsetzung der NIS-2-Richtlinie praxisnäher gestalten.

13. Ablösung Digitaler Dienste durch Digitale Infrastrukturdienste

Im aktuellen Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz - BSIG) sind Anforderungen an Digitale Dienste formuliert. Die Definition der Digitalen Dienste sowie die einschlägigen Anforderungen sind weitestgehend vollständig in den Definitionen sowie zugehörigen Anforderungen der Digitalen Infrastrukturdienste nach §30 (3) im aktuellen Referentenentwurf enthalten. Die diesbezüglichen Regelungen im Gesetz zur Umsetzung der NIS_2-Richtlinie sollten nicht parallel zu den kongruenten Regelungen des BSI-Gesetzes gelten, sondern diese vollständig ablösen. Dies würde die Komplexität der Regelungen sowie den Aufwand ihrer Einhaltung wesentlich erleichtern, ohne das angestrebte Sicherheitsniveau zu reduzieren.

Ansprechpartner

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

Martin Lorenz
Abteilungsleiter Security, Daten & Digitalisierung
martin.lorenz@vda.de

Der Verband der Automobilindustrie (VDA) vereint rund 620 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.

Herausgeber	Verband der Automobilindustrie e. V.(VDA) Behrenstraße 35,10117 Berlin www.vda.de Deutscher Bundestag Lobbyregister-Nr.: R001243 EU-Transparenz-Register-Nr.: 9557 4664 768-90

Version	Juni 2025