VDA Verband der Automobilindustrie

Stellungnahme

Verbändebeteiligung zur Umsetzung der NIS-2-Richtlinie

Mai 2024

1. VDA-Empfehlungen zum Referentenentwurf

Registrierungspflichten
- Für Unternehmen mit Niederlassungen in mehreren EU-Staaten soll eine einzige nationale Bescheinigung ausreichen.
- KRITIS-Betreiber müssen sich zusätzlich beim BSI und Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) registrieren.
- Unternehmensverbände könnten betroffene Unternehmen unterstützen.

Meldepflichten
- Die NIS-2-Richtlinie erhöht die Anzahl der Meldungen und deren Anforderungen. Ein effizientes, digitalisiertes Meldeportal soll eingerichtet werden.
- Das BSI sollte in den meisten Fällen von Zwischenmeldungen absehen, um den Erfüllungsaufwand zu minimieren.
- Gemeinsame Meldung verbundener Unternehmen sollte möglich sein, um Komplexität zu reduzieren.
- Meldungen sollten auch in englischer Sprache und zentral (Once-Only-Prinzip) möglich sein.

Managerhaftung
- Die persönliche Verantwortlichkeit der Geschäftsleitung für Cyber-Risikomanagement wird erweitert, ohne Möglichkeit zur Delegation, dies wird kritisch gesehen.
- Geschäftsführer können persönlich haftbar gemacht werden, was eine erhebliche Ausweitung der Haftung bedeutet.

Umsetzung der Risikomanagementmaßnahmen
- Berechnung des Umsetzungsaufwands für die deutsche Wirtschaft ist unzuverlässig.
- Annahme, dass KRITIS-Unternehmen keinen weiteren Umsetzungsaufwand haben, wird von betroffenen Unternehmen widerlegt.

Streichung der Kategorie „Unternehmen im besonderen öffentlichen Interesse“
- Diese Streichung führt zu einer Vereinfachung und klaren Ausrichtung der Cybersicherheitsregulierung.

Sektoren
- Schwierigkeiten für Unternehmen, mithilfe von Anhang I und II der NIS-2 festzustellen, ob sie betroffen sind. Besondere Unsicherheiten bei Sektoren wie „Digitale Infrastruktur“ und „Verwaltung von Informationstechnologie und Telekommunikation“.

Informationssicherheitsbeauftragter (CISO)
- Möglichkeit einen CISO pro betroffene Einrichtung, der bei der Registrierung benannt werden muss, einzurichten.

Überprüfungsmöglichkeiten der Vertrauenswürdigkeit von Beschäftigten
- Beschäftigte sind Hauptziel für Cyberangriffe, daher müssen technische, organisatorische und operative Maßnahmen ergänzt werden. Unternehmen sollten Sicherheitsüberprüfungen für ihre Beschäftigten beantragen können.

Fehlende Aufnahme öffentlicher Verwaltung
- Öffentliche Verwaltungen der Länder und Kommunen sollten in den Anwendungsbereich aufgenommen werden, da sie essenzielle Verwaltungsdienstleistungen erbringen.

1. Einführung

Der Verband der Automobilindustrie (VDA) bedankt sich für die Möglichkeit, zum aktuellen Referentenentwurf des Bundesministeriums des Innern und für Heimat 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) vom 7. Mai 2024 Stellung nehmen zu können. Wir begrüßen, dass durch die Umsetzung der NIS-2-Richtlinie der Ordnungsrahmen, der durch das Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) von 2015 und dem IT-Sicherheitsgesetz 2.0 von 2021 geschaffen wurde, erweitert und entsprechend angepasst wird.

Infolge der Umsetzung werden insbesondere neue Vorgaben für bestimmte Unternehmen eingeführt, es kommen aber auch Regelungen für die Bundesverwaltung hinzu. Dabei sind aus Sicht des VDA 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 entscheidend.

Angesichts der zunehmenden Cybersicherheitsvorfälle, die auch zahlreiche Städte und Landkreise betreffen, ist eine gut funktionierende öffentliche Verwaltung für Bürger und Wirtschaft von großer Bedeutung, natürlich auch für die deutsche Automobilindustrie. Mit der Ausweitung des Anwendungsbereichs der NIS-2-Richtlinie sind bereits Unternehmen mittlerer Größe betroffen, wodurch auch Landkreise und Städte zur Umsetzung angemessener Cybersicherheitsmaßnahmen verpflichtet werden. Daher fordern wir die Bundesregierung auf, die öffentliche Verwaltung aller Ebenen des Föderalstaats in den Anwendungsbereich einzubeziehen, um sensible Daten besser vor Cyberkriminellen zu schützen.
Es wäre ratsam, dass zur effizienten Durchführung von Penetrationstests auch sog. ethische Hacker notwendig sind, und dass in der nationalen Umsetzung der NIS-2 eine entsprechende Rechtfertigung mit Bezug auf § 202 a StGB eingefügt wird. So könnten Hacker, die mit ethischer Motivation Unternehmen beim Auffinden von Sicherheitslücken unterstützen, durch Schaffung einer ausdrücklichen Regelung straffrei bleiben.

In der **Anlage 2** des Entwurfs wird unter **Nummer 5.5 die Herstellung Kraftwagen und Kraftwagenteilen** namentlich benannt. Somit betrifft dieser Entwurf auch die deutsche Automobilindustrie als Sektor **„wichtige Einrichtung“**.

Die wesentlichen Änderungen des aktuellen Referentenentwurfs beinhalten:

- Die Einführung der Kategorien gemäß der NIS-2-Richtlinie erweitert den Anwendungsbereich deutlich, der bisher auf Betreiber kritischer Infrastrukturen, Anbieter digitaler Dienste und Unternehmen im besonderen öffentlichen Interesse beschränkt war.
- Der Katalog der Mindestsicherheitsanforderungen gemäß Artikel 21 Absatz 2 der NIS-2-Richtlinie wird in das BSI-Gesetz integriert, wobei die Intensität der Maßnahmen entsprechend den verschiedenen Kategorien differenziert wird, um die Verhältnismäßigkeit zu wahren.
- Das bisherige einstufige Meldeverfahren für Vorfälle wird durch das dreistufige Meldesystem der NIS-2-Richtlinie ersetzt, wobei der bürokratische Aufwand für die Einrichtungen im Rahmen des nationalen Umsetzungsspielraums minimiert werden soll.

- Das Instrumentarium des Bundesamts für Sicherheit in der Informationstechnik (BSI) wird im Hinblick auf die von der NIS-2-Richtlinie vorgesehenen Aufsichtsmaßnahmen erweitert.
- Für die Wirtschaft erhöht sich der jährliche Erfüllungsaufwand um rund 2,3 Milliarden Euro. Insgesamt entsteht ein einmaliger Aufwand von rund zwei Milliarden Euro. Dieser ist fast ausschließlich der Kategorie Einführung oder Anpassung digitaler Prozessabläufe zuzuordnen.

3. Zusammenfassung

Im Rahmen der Umsetzung der NIS-2-Richtlinie müssen Unternehmen, die als „besonders wichtig“ oder „wichtig“ eingestuft werden, sich spätestens innerhalb von drei Monaten registrieren. Dies soll über ein offizielles Internetportal erfolgen. Eine bedeutende Maßnahme ist die automatisierte Bereitstellung relevanter Informationen durch staatliche Stellen für die betroffenen Unternehmen.

Um den Verwaltungsaufwand zu minimieren, sollen Unternehmen mit Niederlassungen in mehreren EU-Mitgliedstaaten nur einmalig eine Bescheinigung ihrer nationalen Behörde vorlegen müssen. Verbundene Unternehmen sollen die Möglichkeit haben, sich gemeinsam zu registrieren, da sie häufig gemeinsame Dienste und Infrastrukturen nutzen. Eine solche gemeinsame Registrierung reduziert aus Sicht des VDA den Aufwand und Komplexität sowohl für die Unternehmen als auch für das BSI. Nachteile sind hierbei nicht erkennbar, solange die verbundenen Unternehmen explizit ausgewiesen werden.

Zusätzlich zu den bisherigen Anforderungen des IT-Sicherheitsgesetzes 2.0 müssen sich weitere Unternehmen beim BSI und teilweise beim BBK registrieren, wenn die NIS-2- und CER-Richtlinien für KRITIS-Betreiber in Kraft treten. Diese Registrierungspflichten sollten effizient und digital gestaltet werden, um den Bedürfnissen der Unternehmen gerecht zu werden. Der Zugang staatlicher Stellen sollte nach dem Need-to-know-Prinzip erfolgen. Die Bündelung aller relevanten Informationen zu einem Cybervorfall an einer zentralen Stelle hätte prozessuale Vorteile hinsichtlich Effizienz und Effektivität, sofern angemessene Sicherheitsstandards eingehalten werden.

Angesichts der Vielzahl betroffener Unternehmen sollten Unternehmens- und Branchenverbände diese aktiv unterstützen können.

Die Meldepflichten werden durch die NIS-2-Richtlinie erheblich ausgeweitet. Es ist entscheidend, dass das BSI zusammen mit der Europäischen Kommission und ENISA ein effizientes und vollständig digitalisiertes Meldeportal einrichtet, um die knappen Meldefristen nicht durch Mehrfachmeldungen und unterschiedliche Formerfordernisse zusätzlich zu verkürzen.
Um den erheblichen Erfüllungsaufwand zu berücksichtigen, sollte das BSI von Zwischenmeldungen absehen. Besonders mittelständische Unternehmen benötigen ihre Ressourcen zur Bewältigung bedeutender Sicherheitsvorfälle. Daher sollten unnötige Mehrfachmeldungen vermieden werden. Stattdessen sollte das Beratungsangebot gestärkt und alle Sicherheitsbehörden zur Einbindung bedeutender Einrichtungen verpflichtet werden.

Der VDA unterstützt die Nutzung des Organisationskontos als zentrale Kommunikationsschnittstelle zwischen Staat und Industrie. Dies würde den bürokratischen Aufwand reduzieren und dem Once-Only-Prinzip gerecht werden.

Unternehmen in einem Konzernverbund sollten die Möglichkeit haben, Meldungen zu einem gemeinsamen Sachverhalt in einer einzelnen gemeinsamen Meldung zusammenzufassen, um die Effizienz zu erhöhen und die Bearbeitung zu beschleunigen. Meldungen sollten auch in englischer Sprache möglich sein, um die Arbeit des BSI, zu erleichtern und die Weitergabe von Informationen an internationale Partner zu vereinfachen. Die vorgesehenen Fristen für die Meldepflicht sind für die Automobilindustrie umsetzbar, dennoch sollten sie national und international koordiniert sein.

Es ist unerlässlich, dass eine klare Regelung zur Zusammenarbeit und ein Schutz der Unternehmens- und Kundendaten sichergestellt werden, besonders im Hinblick auf die Melde- und Dokumentationspflichten bei Cybervorfällen. Kleine und mittlere Unternehmen (KMU) benötigen eine unbürokratische Umsetzung und Anwendung des Meldewesens, da sie oft Schwierigkeiten haben, die Pflichten fristgerecht zu erfüllen. Eine zentrale Anlaufstelle für Meldungen auf Bundesebene sollte eingerichtet werden, um das Once-Only-Prinzip zu ermöglichen. Das BSI könnte als Knotenpunkt für die Zusammenarbeit zwischen Bund und Ländern dienen.

Der aktuelle Referentenentwurf erweitert in §30 die persönliche Verantwortlichkeit der Geschäftsleitung für das Cyber-Risikomanagement erheblich. Geschäftsleiter können persönlich haftbar gemacht werden, was eine deutliche Ausweitung der Haftung bedeutet.

In der deutschen Gesetzgebung fehlen detaillierte Vorgaben für Unternehmen und Behörden zur Umsetzung der in NIS-2 Artikel 21 genannten Risikomanagementmaßnahmen, insbesondere hinsichtlich Kritikalität, Sektor und Unternehmensgröße. Die Berechnung des wirtschaftlichen Aufwands ist unzuverlässig, da Annahmen wie kein zusätzlicher Aufwand für KRITIS-Unternehmen und 17% der Unternehmen ohne Umsetzungsbedarf angezweifelt werden. Dringend notwendig sind eine detaillierte Umsetzungshilfe und klare Erwartungen seitens des BSI, um Unternehmen eine fristgerechte Umsetzung zu ermöglichen. Eine präzisere Herleitung der Umsetzungskosten und eine Handreichung des BSI würden den betroffenen Unternehmen erheblich helfen.

Unternehmen haben Schwierigkeiten festzustellen, ob sie gemäß Anhang I und II der NIS-2 betroffen sind, mit Ausnahme der Automobilbranche, für die dies einfacher ist. Unternehmen können in mehreren Sektoren betroffen sein und müssen dies bei der Registrierung angeben. Große Unsicherheit besteht bei Sektoren wie „Digitale Infrastruktur“ und „Verwaltung von Informationstechnologie und Telekommunikation“. Beispielsweise könnten deutsche Muttergesellschaften, die europäischen Tochtergesellschaften Rechenzentrumsdienste anbieten, als „Wesentliche Einrichtungen“ gelten. Ebenso könnten alle Einrichtungen, die SOC-Dienstleistungen anbieten, NIS-2-relevant sein, was auch ausländische Tochterunternehmen betreffen könnte. Eine Klarstellung in diesen Sektoren würde den Unternehmen helfen, sich angemessen vorzubereiten.

Sicherheitsüberprüfungen für Beschäftigte sollten ermöglicht und effizient gestaltet werden, wobei rechtliche Anpassungen im Bundesdatenschutzgesetz erforderlich sein könnten. Ausreichende Ressourcen müssen auf staatlicher Seite bereitgestellt werden.

Auf Bundesebene wird ein „CISO-Bund“ eingeführt. Im Rahmen der NIS-2-Umsetzung könnte jede betroffene Einrichtung einen verantwortlichen CISO benennen, ähnlich wie Datenschutzbeauftragte. Der Gesetzgeber kann sich dabei an den BAIT-Vorgaben (Bankaufsichtliche Anforderungen an die IT) orientieren. Die Geschäftsleitung muss einen Informationssicherheitsbeauftragten einsetzen, der für alle Belange der Informationssicherheit verantwortlich ist, sowohl intern als auch gegenüber Dritten.

Diese Funktion soll getrennt vom IT-Betrieb und der IT-Entwicklung sein, um Interessenkonflikte zu vermeiden und die umfangreiche Aufgabe des Informationssicherheitsbeauftragten zu unterstreichen.

Öffentliche Verwaltungen der Länder und Kommunen sollten ebenfalls in den Anwendungsbereich aufgenommen werden, da sie essenzielle Verwaltungsdienstleistungen erbringen.

Der VDA begrüßt die Streichung der Kategorie „Unternehmen im besonderen öffentlichen Interesse“, da dies zu einer klaren Ausrichtung der Cybersicherheitsregulierung führt. Schwellenwerte für Kritische Anlagen sollten direkt im Gesetz festgelegt werden, um Transparenz und eine klare Orientierung für betroffene Unternehmen zu gewährleisten.

Im Einzelnen:

4. Registrierungspflichten

Im Rahmen der Umsetzung der NIS-2-Richtlinie wird von jedem Unternehmen erwartet, dass besonders wichtige und wichtige Einrichtungen sich spätestens nach drei Monaten registrieren (§33, §34 des aktuellen Referentenentwurfs). Es wird voraussichtlich ein offizielles Internetportal für die Registrierung geben. Eine entscheidende Voraussetzung ist die automatisierte Bereitstellung relevanter Informationen seitens der staatlichen Stellen für die betroffenen Unternehmen.

Um den Verwaltungsaufwand für betroffene Unternehmen mit Niederlassungen in anderen EU-Mitgliedstaaten zu minimieren, sollten diese nur einmalig eine Bescheinigung ihrer jeweiligen nationalen Behörde vorlegen müssen, welche die europaweite Unternehmensstruktur und die einzelnen Ländergesellschaften beinhaltet, die von den zuständigen Behörden akzeptiert und an die betroffenen Behörden anderer europäischer Länder weitergeleitet wird.

Für Unternehmen in einem (Konzern-)Verbund sollte eine Registrierung der verbundenen Unternehmen in einem einzelnen gemeinsamen Registrierungsvorgang ermöglicht werden. Verbundene Unternehmen nutzen zumeist gemeinsame Dienste, Infrastrukturen, Systeme, Anwendungen, Prozesse und Verfahren. Eine Zusammenfassung der Registrierung einzelner verbundener Unternehmen in einer gemeinsamen Registrierung reduziert den Aufwand und Komplexität für die betroffenen Unternehmen und das BSI. Nachteile einer gemeinsamen Registrierung verbundener Unternehmen sind nicht erkennbar, solange die gemeinsame Registrierung die zu registrierenden verbundenen Unternehmen explizit ausweist.

Mit dem gleichzeitigen Inkrafttreten und der Umsetzung der NIS-2-Richtlinie sowie der CER-Richtlinie für KRITIS-Betreiber werden zusätzliche Unternehmen neben den bisherigen Anforderungen des IT-SiG 2.0 sich beim BSI und teilweise auch beim BBK registrieren müssen. Diese Registrierungspflichten sollten an die Bedürfnisse der Unternehmen angepasst und möglichst effizient und digital gestaltet sein. Der Zugang der staatlichen Stellen sollte nach dem Need-to-know-Prinzip erfolgen. Die Bündelung aller relevanten Informationen zu einem Cybervorfall an einer zentralen Stelle hätte prozessuale Vorteile hinsichtlich Effizienz und Effektivität, sofern angemessene Sicherheitsstandards für die Informationsübertragung und -speicherung eingehalten werden.

Aufgrund der erwarteten Vielzahl betroffener Unternehmen sollte aus unserer Sicht in Betracht gezogen werden, dass Unternehmens- und Branchenverbände aktiv auf Unternehmen zugehen und ggf. unterstützen könnten.

Die Reduzierung der Frist bei Änderungen auf zwei Wochen gegenüber der Frist in der NIS-2 von 3 Monaten stellt eine deutliche Erschwerung für deutsche Unternehmen dar und sollte zurückgenommen werden.

5. Meldepflichten

Vor dem Hintergrund der massiven Ausweitung der Meldepflichten, die im NIS2UmsuCG vorgesehen sind (von einer Meldung pro Vorfall gemäß IT-Sicherheitsgesetz 2.0 zu bis zu fünf Meldungen, von tatsächlichen Vorfällen gemäß IT-Sicherheitsgesetz 2.0 zu möglichen Vorfällen), ist es von entscheidender Bedeutung, dass das Bundesamt für Sicherheit in der Informationstechnik (BSI) in Zusammenarbeit mit der Europäischen Kommission, der Europäischen Agentur für Cybersicherheit (ENISA) und unter Einbeziehung des BBK ein effizientes und vollständig digitalisiertes Meldeportal einrichtet. Dieses Portal soll sicherstellen, dass die ohnehin knappen Meldefristen durch Mehrfachmeldungen und unterschiedliche Formerfordernisse nicht zusätzlich verkürzt werden.

Um den erheblichen Erfüllungsaufwand, der mit jeder Meldung verbunden ist, zu berücksichtigen, sollte das BSI in den meisten Fällen von einer Zwischenmeldung gemäß § 32 Abs. 1 Nr. 3 absehen. Insbesondere mittelständische Unternehmen werden während der Bearbeitung eines bedeutenden Sicherheitsvorfalls all ihre personellen und finanziellen IT-Sicherheitsressourcen in die Bewältigung des Vorfalls investieren müssen. Daher ist es unerlässlich, unnötige Mehrfachmeldungen zu vermeiden, um die Unternehmen nicht zusätzlich zu belasten. Stattdessen sollte das Beratungsangebot gemäß § 36 Abs. 1 gestärkt und alle Sicherheitsbehörden zur Einbindung bedeutender Einrichtungen verpflichtet werden.

Der VDA unterstützt die Nutzung des im Rahmen des Onlinezugangsgesetzes entwickelten Organisationskontos als Portallösung für die Meldung. Dies würde den bürokratischen Aufwand in den Unternehmen erheblich reduzieren, da das Organisationskonto als zentrale Kommunikationsschnittstelle zwischen Staat und Wirtschaft dienen könnte. Eine einheitliche Schnittstelle zwischen Staat und Wirtschaft würde auch die Umsetzungskosten erheblich senken, da nur ein System gepflegt und weiterentwickelt werden müsste. Darüber hinaus würde die Nutzung des Organisationskontos dem Once-Only-Prinzip gerecht werden.

Zur Reduktion der Komplexität des Meldeverfahrens und zur Begrenzung der Aufwand des BSI und betroffener Unternehmen sollte Unternehmen in einem (Konzern-)Verbund ermöglicht werden, Meldungen der verbundenen Unternehmen zum gleichen Sachverhalt und zur Erfüllung gleichartiger Meldepflichten der einzelnen verbundenen Unternehmen zu einer gemeinsamen Meldung zusammenzufassen. Durch die gemeinsame Meldung geht keine Information verloren. Stattdessen gewinnen sowohl die Erstellung als auch die Weiterleitung und Bearbeitung von Meldungen deutlich an Transparenz, Effizienz, Geschwindigkeit und Sicherheit sowohl auf Seiten der betroffenen Unternehmen als auch auf Seiten des BSI.

Um international tätigen Unternehmen, deren Cybersecurity-Teams häufig Englisch sprechen, entgegenzukommen, sollte die Möglichkeit geschaffen werden, Meldungen auch in englischer Sprache an das BSI abzugeben. Dies würde nicht nur die Arbeit des BSI erleichtern, sondern auch die Weitergabe von Informationen an internationale Partner vereinfachen. Die vorgeschlagenen Fristen für die Meldepflicht gemäß §32 sollten für die Automobilindustrie umsetzbar sein. Die Meldepflichten sollten jedoch national und international koordiniert sein, um einen reibungslosen Ablauf zu gewährleisten.

Es ist unerlässlich, eine klare Regelung zur Zusammenarbeit und eine Verpflichtung der Behörden zum Schutz der Unternehmens- und Kundendaten sicherzustellen, insbesondere im Hinblick auf die vorgeschriebenen Melde- und Dokumentationspflichten von Cybervorfällen durch die betroffenen Unternehmen gegenüber den zuständigen Behörden wie dem BSI und dem BBK.

Angesichts der Tatsache, dass gerade kleine und mittlere Unternehmen (KMU) in der Automobilindustrie in vielen Fällen Schwierigkeiten haben werden, die vorgeschriebenen Pflichten innerhalb der gesetzlich definierten Fristen zu erfüllen, ist eine unbürokratische Umsetzung und Anwendung des Meldewesens dringend erforderlich. Gemäß der NIS-2-Richtlinie (und auch gemäß der CER-Richtlinie) sollte für Cybervorfälle eine einzige Anlaufstelle auf Seiten der Bundesbehörden benannt werden, um eine einmalige Meldung oder Berichterstattung pro Vorfall zu ermöglichen (Once-Only-Prinzip). Das BSI könnte dabei als Knotenpunkt für die Zusammenarbeit zwischen Bund und Ländern dienen und kollaborative IT-Anwendungen für den Informationsaustausch und das Meldeverfahren nutzen. 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-Mitgliedstaaten berichten müssen, um den Aufwand für Unternehmen und Behörden zu minimieren. Alternativ vorstellbar wäre eine Meldung an die länderübergreifende Behörde ENISA bei länderübergreifenden Vorfällen von multinationalen Konzernen.

Auf Basis der EU General Safety Regulation existiert bereits eine Berichtspflicht für die Automobilindustrie gegenüber nationalen Behörden. Hier sollte sichergestellt sein, dass eine Berichtspflicht über die gleichen Aspekte an verschiedene nationale Behörden vermieden wird.

6. Managerhaftung

Der aktuelle Referentenentwurf geht über die Vorgaben der NIS-2-Richtlinie hinaus, indem er die persönliche Verantwortlichkeit der Geschäftsleitung für die Überwachung des Cyber-Risikomanagements, insbesondere für besonders wichtige und wichtige Einrichtungen, ohne die Möglichkeit der Delegation dieser Verantwortung an Dritte vorsieht (§38). Demnach können Geschäftsleiter persönlich für Schäden durch Cyberrisiken haftbar gemacht werden, was Regressansprüche und Bußgeldforderungen betrifft. Ein Verzicht auf Schadenersatz-forderungen gegenüber den Geschäftsleitern oder ein Vergleich ist nur im Falle einer Insolvenz zulässig. Dies bedeutet eine erhebliche Ausweitung der persönlichen Haftung von Geschäftsleitern, insbesondere in Gesellschaften mit beschränkter Haftung (GmbHs), die rechtlich bisher einen gewissen Spielraum hatten.

Es bleibt unklar, ob diese persönliche Haftung versicherbar ist, und welche Schritte seitens der Aufsichtsräte, der Behörden und der Staatsanwaltschaft eingeleitet werden, wenn die Binnenhaftung nicht oder nur in Teilen eingefordert wird (Verstoß gegen § 38 (2)). Es wäre zu begrüßen, wenn diese Punkte im Gesetz verdeutlicht werden würden und dies nicht der Auslegung der Juristen bedarf.

7. Umsetzung der Risikomanagementmaßnahmen

In der deutschen Gesetzgebung kommt es zu keiner Detaillierung der Erwartungshaltung gegenüber den Unternehmen und Behörden wie genau die in NIS-2 Artikel 21 erwähnten Risikomanagementmaßnahmen in Bezug auf Kritikalität, Sektor, Unternehmensgröße und weiteren Faktoren anzuwenden sind.

Die Berechnung des Aufwands für die deutsche Wirtschaft könnte ein grober Anhalt für den Umsetzungsaufwand sein. Stellt jedoch keine verlässliche Informationsquelle dar. Bspw. wird angenommen, dass KRITIS-Unternehmen keinen weiteren Aufwand zur Umsetzung der NIS-2 hätten. Rückfragen bei betroffenen Unternehmen bezeugen das Gegenteil. Auch die Annahme, 17% der Unternehmen hätten keinen weiteren Umsetzungsbedarf, darf stark angezweifelt werden. Die Gleichsetzung des Aufwands für die Umsetzung der NIS-Richtlinie mit dem Aufwand zur Umsetzung der NIS2-Richtlinie ist nicht haltbar. Einzig die Annahme, dass 70% bei großen wichtigen Einrichtungen im Vergleich zu einer wesentlichen Einrichtung und 35% bei einer mittleren wichtigen Einrichtung im Vergleich zu einer wesentlichen Einrichtung einzuhalten ist, stellt einen groben Anhaltspunkt der Erwartungshaltung des Gesetzgebers dar.
Eine Umsetzungshilfe erstellt durch das BSI mit konkreten Erwartungshaltungen gegenüber den betroffenen Einrichtungen in dem Umfang der umzusetzenden Maßnahmen ist dringend notwendig, um den Unternehmen die Möglichkeit zu geben diese fristgerecht umzusetzen.

Eine deutlich bessere Herleitung der Umsetzungskosten für die betroffenen Unternehmen sowie eine Handreichung des BSI zu den erwarteten Maßnahmen würde eine deutliche Hilfe für die betroffenen Unternehmen darstellen.

8. 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 NIS2UmsuCG 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.

9. 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.

10. 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 Datenschutzbeauftragten 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 Informationssicherheitsbeauftragten 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.

11. 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.

12. 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.

Ansprechpartner

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

Martin Lorenz
Abteilungsleiter komm. Fahrzeugtechnologien & Eco-Systeme
Fachgebietsleiter Cybersecurity, Daten & Wirtschaftsschutz
martin.lorenz@vda.de

Timm Haußen
Referent
timm.haussen@vda.de

Der Verband der Automobilindustrie (VDA) vereint mehr als 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 Wirschafts- 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	Mai 2024