VDA Verband der Automobilindustrie

Kurzbewertung

Wirtschaftsbezogene Regelungen zur Umsetzung der NIS 2 Richtlinie in Deutschland

Inhaltsangabe

Berlin, Oktober 2023

1 Harmonisierung mit NIS 2 Richtlinie

Der VDA begrüßt die Harmonisierung der in der NIS 2 Richtlinie eingeführten Kategorien „essential entities“ und „important entities“ mit den zuvor geltenden Kategorien aus dem IT-Sicherheitsgesetz 2.0, „Kritische Infrastrukturen“ und „Unternehmen im besonderen öffentlichen Interesse“. Diese werden zukünftig gemäß §28 Abs.1 und Abs.2 im Diskussionspapier in „besonders wichtige“ und „wichtige“ Einrichtungen unterschieden. Darüber hinaus begrüßen wir die Entscheidung, auf die zusätzliche Klassifizierung gemäß Referentenentwurf vom 3. Juli 2023 NIS2UmsuCG nach „Großunternehmen“ und „mittleren Unternehmen“ zu verzichten.

Unklar hingegen bleibt, warum mit den Bezeichnungen „besonders wichtige Einrichtungen“ und „wichtige Einrichtungen“ von der NIS 2 Richtlinie abgewichen wird. In der deutschsprachigen Ausgabe der NIS 2 Richtlinie wird die englische Vorgabe „essential entities“ mit „wesentliche Einrichtungen“ übersetzt und „important entities“ mit „wichtige Einrichtungen“ übersetzt. Gleiches gilt für die Terminologie „Betreiber kritischer Anlagen“. In der CER-Richtlinie (EU 2022/2557) als auch in der NIS 2 Richtlinie (EU 2022/2555) ist jeweils die Rede von einer „kritischen Einrichtung“.

Der VDA plädiert dafür, an den auf europäischer Ebene definierten Begrifflichkeiten festzuhalten. Diese sind eingeführt und etabliert. Durch die in weiten Teilen bereits jahrelange Nutzung sowie EU-weite Harmonisierung verfügen diese über Anerkennung und stellen somit den Stand der Technik in der Begrifflichkeit dar. Zudem kann durch die Beibehaltung der Begrifflichkeit vermieden werden, dass es bei Übersetzungen zu ungewollten Abweichungen kommt.

besonders wichtige Einrichtung	**wichtige Einrichtung**
▪ Anlage 1: Sektoren mit hoher Kritikalität	▪ Anlage 1: Sektoren mit hoher Kritikalität ▪ Anlage 2: Sonstige kritische Sektoren
▪ ab 250 Mitarbeiter ▪ Jahresumsatzbilanz ab 50 Mio. € ▪ Jahresbilanzsumme ab 43 Mio. €	▪ ab 50 Mitarbeiter ▪ Jahresumsatzbilanz ab 10 Mio. € ▪ Jahresbilanzsumme ab 10 Mio. €
▪ Betreiber kritischer Anlagen	▪ Vertrauensdienstanbieter
▪ Qualifizierter Vertrauensdienstanbieter, Top Level Domain Name Registries, DNS-Dienstanbieter	
▪ Telekommunikationsdienstleiter ab 50 MA, ab 10 Mio. € Jahresumsatz und ab 10 Mio. € Jahresbilanzsumme	

2 Risikomanagementmaßnahmen durch Dritte

Der §38 mit der Bezeichnung „Billigungs-, Überwachungs- und Schulungspflicht für Geschäftsleiter besonders wichtiger und wichtiger Einrichtungen“ besagt, dass Geschäftsleiter verpflichtet sind, Risikomaßnahmen im Bereich der Cybersecurity zu billigen und ihre Umsetzung zu überwachen.

Im vorangegangenen Referentenentwurf war es dem Geschäftsleiter nicht gestattet diese Aufgabe an dritte zu übertragen. Dieses Verbot wurde nun im §38 (1) gestrichen. Der VDA begrüßt grundsätzlich diese Streichung, da nun die Möglichkeit besteht, dass Geschäftsleitungen diese Verantwortlichkeit an qualifiziertes Fachpersonal auslagern können. Dieser Schritt hat zur Konsequenz, dass keine zusätzlichen internen Ressourcen gebunden werden müssen und gleichzeitig auf das Fachwissen, welches auf dem Markt verfügbar ist, zurückgegriffen werden kann. Dies wiederum ermöglicht eine beschleunigte und nachhaltigere Umsetzung der Ziele zur Steigerung der Resilienz. Gleichwohl sollte die übergreifende Verantwortung bei der Geschäftsleitung bestehen bleiben, wie es im Diskussionspapier vorgesehen ist.

3 Enthebung von Leitungsfunktion

Sehr kritisch hingegen sieht der VDA den §64 (10), wonach es dem Bundesamt für Sicherheit in der Informationstechnik (BSI) gestattet ist, natürlichen Personen in der Rolle der Geschäftsführung oder der gesetzlichen Vertretung für Leitungsaufgaben ihrer Rolle zu entheben. Dies kann gemäß dem Diskussionspapier der Fall sein, wenn Fristen zur Umsetzung von Anordnungen seitens des BSI nicht eingehalten werden. Diese Regelung kann bei komplexen Konzernstrukturen zu massiven Problemen führen. Demnach könnten Konzernchefs bzw.- chefinnen, bei denen Teile des Konzerns als „besonders wichtig“ eingestuft werden, ihrer Leitungsfunktion enthoben werden, auch wenn die betroffenen Bereiche nicht das Kerngeschäft bilden.
Die Maßnahme wäre unverhältnismäßig und muss aus dem aktuellen Diskussionspapier gestrichen werden. Der VDA fordert daher die ersatzlose Streichung dieses Absatzes.

4 Mitarbeiterüberprüfung

Kritisch sieht der VDA, dass erneut unsere Forderung nach einem rechtssicheren Rahmen für die Vertrauenswürdigkeitsprüfung von Personal, mit sicherheitskritischen Aufgaben erneut nicht berücksichtigt wurde. Ohne die gesetzliche Möglichkeit, Personal mit sicherheitskritischen Aufgaben einer angemessenen Vertrauenswürdigkeitsprüfung zu unterziehen, kann eine gesteigerte Resilienz und Sicherheit kritischer Anlagen nicht erreicht werden. Der Schutz vor digitalen Risiken gelingt nur im Zusammenspiel von technischen, organisatorischen und personellen Maßnahmen. Zukünftig sollten alle Unternehmen, die dem Anwendungsbereich des NIS 2 Umsetzungsgesetzes 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 Umsetzungsgesetzes einführen. Eine ausschließliche Fokussierung auf technische Sicherheit ist nicht zielführend.

5 Behandlung verbundener Unternehmen

Die Einstufung von verbundenen Unternehmen in besonders wichtige, wichtige oder kritische Einrichtungen erfolgt für das jeweilige Einzelunternehmen im Konzernverbund. Verbundene Unternehmen können gemeinsame Meldungen, Berichte und Erklärungen gegenüber der zentralen Melde- und Kontaktstelle abgeben. Daher fordern wir, dass eine Registrierung und Abgabe von Meldungen auch durch den Konzernverbund für die Einzelgesellschaften summarisch möglich sind.

6 Meldepflichten

Hinsichtlich Meldepflichten muss sichergestellt werden, dass für verbundene Unternehmen zu einem Vorfall Meldungen nicht an Meldestellen in mehreren Ländern der Europäischen Union abgegeben werden müssen.

Hilfsweise sollten für verbundene Unternehmen Meldepflichten dahingehend eingeschränkt werden, dass Meldungen zu Sicherheitsvorfällen unterlassen werden können, wenn eine Meldung in einem anderen Land der Europäischen Union gemäß den dort geltenden gesetzlichen Vorgaben erfolgt. Zielführend wäre, wenn eine Meldung konzernweit in einem Land der Europäischen Union abgegeben werden kann.

7 Aufsichts- und Durchsetzungsmaßnahmen

Bedient sich das BSI bei der Überprüfung der Einhaltung von Anforderungen eines Dritten, so können Gebühren und Kosten von der geprüften Einrichtung nur dann erhoben werden, wenn das Bundesamt auf Grund von Anhaltspunkten tätig geworden ist, die berechtigte Zweifel an der Einhaltung der **Anforderungen begründen und die Überprüfung** die mangelnde Einhaltung der Anforderungen bestätigt.

Ansprechpartner

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

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

Timm Haußen
IT-Projektleiter
Security & Daten
timm.haussen@vda.de

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.

Herausgeber	Verband der Automobilindustrie e.V. (VDA) Behrenstraße 35, 10117 Berlin www.vda.de Registrierter Interessenvertreter - R001243
Copyright	Verband der Automobilindustrie e.V. (VDA) Nachdruck und jede sonstige Form der Vervielfältigung ist nur mit Angabe der Quelle gestattet.
Version	Version 1.0, Oktober 2023