

# NIS2UmsuCG – Stellungnahme DEKRA

DEKRA Konzernrepräsentanz, 10117 Berlin, Behrenstr. 29

Dr. Fabienne Beez  
DEKRA  
Konzernrepräsentanz  
Behrenstr. 29  
10117 Berlin  
Telefon (030) 98 60 98 8 10  
E-Mail buero-berlin@dekra.com

Berlin, im Mai 2024

**DEKRA Positionierung zum Entwurf eines Gesetzes des Bundesministeriums des Innern und für Heimat zur „Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung“ (NIS-2-Umsetzung und Cybersicherheitsstärkungsgesetz NIS2UmsuCG)**

Sehr geehrter Herr ,  
sehr geehrte Damen und Herren,

im vergangenen Jahr kosteten Cyberattacken auf Hard- und Software die Weltwirtschaft 8 Billionen US Dollar<sup>1</sup>. BITKOM beziffert die Schäden allein in Deutschland auf 203 Mrd. EUR p.a. Laut BSI-Lagebericht der IT-Sicherheit in Deutschland 2023 zeigte sich im aktuellen Berichtszeitraum national eine angespannte bis kritische Lage. Die Bedrohung im Cyberraum ist damit so hoch wie nie zuvor.

Mit seiner knapp hundertjährigen Erfahrung und rund 49.000 Mitarbeiter:innen ist DEKRA eine der weltweit führenden, unabhängigen Prüf- und Expertenorganisationen. Im Hinblick auf Cybersecurity setzen wir uns für ein höchstmögliches Sicherheitsniveau ein und unterstützen Unternehmen dabei ihre digitale Infrastruktur zu schützen – sei es im Rahmen der Umsetzung der Richtlinien zur Netzwerk- und Informationssicherheit (NIS-1 und NIS-2) oder des Cyber Resilience Acts (CRA).

Die DEKRA Cybersicherheitsdienstleistungen decken in diesem Zusammenhang den gesamten Produktlebenszyklus ab und umfassen die Prüfung, Bewertung und

---

<sup>1</sup> [US Agency for International Development, 2023](#)

Datum Berlin, im Mai 2024  
E-Mail buero-berlin@dekra.com  
Telefon 030-98609880

DEKRA  
Konzernrepräsentanz Berlin  
Behrenstr. 29, 11017 Berlin  
[www.dekra.de](http://www.dekra.de)

Zertifizierung nach allgemein anerkannten Cybersicherheitsstandards wie Common Criteria (ISO 15408), FIPS 140-3 (ISO 19790), eIDAS regulation, LINCE oder GSMA - NESAS 3GPP; sowie im Kontext spezifischer Sicherheitsstandards, wie IEC 62443, ISO 21343 oder UL2600. DEKRA validiert branchen- und sektorenübergreifend die Cybersecurity von Produkten und Anwendungen für die Zulieferer globaler Tech-Unternehmen. Als eine der ersten akkreditierten Zertifizierungsstellen in Deutschland bietet DEKRA Cybersecurity-Dienstleistungen für Automobilhersteller an.

Wir bedanken uns für die Möglichkeit zu einer Stellungnahme im Rahmen der Konsultation zum NIS-2-Diskussionspapier sowie unserer Teilnahme am Werkstattgespräch „Wirtschaftsbezogene Regelungen zur Umsetzung der NIS-2-Richtlinie in Deutschland“ am 26. Oktober 2023 in Berlin. Sehr gern möchten wir heute die Gelegenheit ergreifen, zum Referentenentwurf „Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung“ Stellung zu nehmen.

### **Nachstehende Anmerkungen sind aus unserer Sicht zentral:**

Die nationale Umsetzung der NIS-2 Richtlinie ist eine wichtige Stellschraube zum Schutz der digitalen Infrastrukturen in Deutschland. DEKRA begrüßt ausdrücklich die signifikante Ausweitung des bisher gültigen Anwendungsbereiches von Cybersicherheitsanforderungen an staatliche und wirtschaftliche Akteure, die wesentliche Dienste erbringen oder Tätigkeiten ausüben. Im Sinne einer europäisch harmonisierten, widerstandsfähigen digitalen Infrastruktur leistet DEKRA einen wesentlichen Beitrag zu einem höchstmöglichen Cybersicherheitsniveau. Hierdurch können nachgelagerte Behörden unterstützt und entlastet werden. Indem wir zur sicheren IT-Anwendungen beitragen, fungiert DEKRA als Enabler für Innovationen. Entscheidend ist dabei, dass die TIC-Branche als unabhängiger Akteur im Rechtsrahmen fest verankert wird.

- DEKRA begrüßt vor diesem Hintergrund insbesondere Artikel 1, § 14, §54 und §65 die für die Zertifizierung bzw. Aufsichts- und Durchsetzungsmaßnahmen das Hinzuziehen anerkannter sachverständiger Stellen bzw. qualifizierter unabhängige Dritter vorsehen.
  - In §54 sollte dabei spezifiziert werden, für welche „bestimmte[n] Produkte und Leistungen“ anerkannte sachverständige Stellen hinzugezogen werden können, bzw. müssen. DEKRA als unabhängige Dritte Stelle verfügt hierbei über ein umfassendes Serviceportfolio in den Bereichen Training, Consulting, Auditierung, Product Testing und Certification. Diese finden Anwendung in den Dienstleistungsbereichen Automotive, Industrial IOT, Medical Devices, FMCG oder ICT.

- Für §14 (1) schlägt DEKRA weiterhin folgende Formulierungsänderung vor: „Das Bundesamt kann zur Erfüllung seiner Aufgaben nach § 3 Absatz 1 Satz 2 Nummer 1, 20, 21, 24 oder 25 auf dem Markt bereitgestellt oder zur Bereitstellung auf dem Markt vorgesehene informationstechnische Produkte und Systeme untersuchen. Es ~~kann~~ **soll** sich hierbei der Unterstützung Dritter bedienen, soweit berechnigte Interessen des Herstellers der betroffenen Produkte und Systeme dem nicht entgegenstehen.“
- Nach § 55 (Konformitätsbewertung und Konformitätserklärung) kann das Bundesamt für die vom Bundesamt in einer Technischen Richtlinie festgelegten Anforderungen und Vorgaben die Durchführung einer Selbstbewertung der Konformität unter der alleinigen Verantwortung des Herstellers oder Anbieters von IKT-Produkten, -Diensten und -Prozessen, einer Person oder einem IT-Sicherheitsdienstleisters, die keine Verbraucherprodukte nach § 57 sind, zulassen. „Der Hersteller oder Anbieter von IKT-Produkten, -Diensten und -Prozessen, die Person oder der IT-Sicherheitsdienstleister kann unter den Voraussetzungen von Satz 1 eine Konformitätserklärung ausstellen, die bestätigt, dass die Erfüllung der in der Technischen Richtlinie festgelegten Anforderungen nachgewiesen wurde. Durch die Ausstellung einer solchen Erklärung übernimmt der Hersteller oder Anbieter der IKT-Produkte, -Dienste und -Prozesse, die Person oder der IT-Sicherheitsdienstleister (Aussteller) die Verantwortung dafür, dass das IKT-Produkt, der IKT-Dienst, der IKT-Prozess, die Person oder die IT-Sicherheitsdienstleistung der Technischen Richtlinie festgelegten Anforderungen entspricht.“
  - Wir begrüßen ausdrücklich, dass die Erbringer von Bestätigungsdienstleistungen im Rahmen des NIS-2-Umsetzungsgesetzes berücksichtigt werden sollen. Zugleich sollte in § 55 (1) die Einbindung unabhängiger Dritter Stellen vorgesehen werden. Die Durchführung einer Selbstbewertung in alleiniger Verantwortung u.a. seitens der Hersteller würde das bestehende und bewährte Prinzip unabhängiger Konformitätsbewertungsprozesse, die durch neutrale Stellen durchgeführt werden, unterminieren. Vor diesem Hintergrund schlägt DEKRA die folgende Formulierung vor:

*(1) „Das Bundesamt kann für die vom Bundesamt in einer Technischen Richtlinie festgelegten Anforderungen und Vorgaben die Durchführung einer Selbstbewertung der **Konformität durch Einbeziehung unabhängiger Dritter Bestätigungsdienstleister** ~~unter der alleinigen Verantwortung~~ des Herstellers oder Anbieters von IKT-Produkten -Diensten und -Prozessen, einer Person oder*

*einem IT-Sicherheitsdienstleisters, die keine Verbraucherprodukte nach § 57 sind, zulassen.“*

*„7. die Befristung der Konformitätserklärung. (3) Wird in den Vorgaben nach Absatz 2 festgelegt, dass die Angaben der Konformitätserklärung nur durch eine akkreditierte Konformitätsbewertungsstelle belegt werden kann, so ~~kann~~ soll das Bundesamt auf Antrag Konformitätsbewertungsstellen, die im Anwendungsbereich dieses Paragraphen tätig werden, eine Befugnis erteilen, als solche tätig zu werden, wenn die maßgeblichen Voraussetzungen der Technischen Richtlinie erfüllt sind. Ohne eine Befugniserteilung durch das Bundesamt dürfen Konformitätsbewertungsstellen im Anwendungsbereich dieses Paragraphen nicht tätig werden.“*

- Gem. Artikel 1, § 57 wird ein freiwilliges IT-Sicherheitskennzeichen eingeführt. DEKRA begrüßt, dass die Plausibilitätsprüfung hierbei auch durch einen vom Bundesamt beauftragten qualifizierten Dritten erfolgen kann. Eine Beteiligung neutraler, unabhängiger Prüfstellen, die direkt am betroffenen Unternehmen agieren, trägt in diesem Zusammenhang zur transparenten und unabhängigen Widerspiegelung der IT-Sicherheit in betroffenen Unternehmen bei.
  - Aus Sicht von DEKRA sollte das IT-Sicherheitskennzeichen im Sinne eines höchstmöglichen Cybersicherheitsniveaus und des Verbraucher:innenschutzes jedoch verpflichtend sein. Die durch das BSI definierten IT-Sicherheitsanforderungen sollten darüber hinaus durch eine Aktualisierung der Technischen Richtlinien kontinuierlich dem jeweiligen Stand der Technik angepasst werden. Nur so kann aktuellen technischen Entwicklungen Rechnung getragen werden und die Zielsetzung des Sicherheitskennzeichens zu mehr Verbraucherschutz fortlaufend gesichert werden.
- Gem. Art. 1, § 31 (2) werden Betreiber kritischer Anlagen dazu verpflichtet, Systeme zur Angriffserkennung einzusetzen. Dabei soll der Stand der Technik eingehalten werden.
  - Eine verpflichtende Zertifizierung dieser Systeme durch qualifizierte, unabhängige Dritte würde hierbei zu einem höchstmöglichen Sicherheitsniveau beitragen.
- Art. 1, § 38 sieht die regelmäßige Teilnahme von Geschäftsleitungen besonders wichtiger Einrichtungen und wichtiger Einrichtungen an Schulungen vor, um ausreichende Kenntnisse und Fähigkeiten zur

Erkennung und Bewertung von Risiken sowie Risikomanagementpraktiken im Bereich der Sicherheit in der Informationstechnik zu erwerben.

- Die Zertifizierung und Durchführung dieser Schulungen durch qualifizierte, unabhängige Dritte würde dabei zu einem höchstmöglichen Sicherheitsniveau beitragen.
- Art. 1, § 39, sieht vor, dass Betreiber kritischer Anlagen die Erfüllung der Anforderungen auf geeignete Weise nachzuweisen haben. Der Nachweis kann durch Sicherheitsaudits, Prüfungen oder Zertifizierungen erfolgen.
  - Sicherheitsaudits, Prüfungen oder Zertifizierungen durch qualifizierte, unabhängige Dritte würden hierbei zu einem höchstmöglichen Sicherheitsniveau beitragen.
- Art. 1, § 43 (2) sieht die regelmäßige Teilnahme der Einrichtungsleitung an Schulungen vor, um ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken sowie Managementpraktiken im Bereich der Informationssicherheit und deren Auswirkungen auf die von der Einrichtung erbrachten Dienste zu erwerben.
  - Die Zertifizierung und Durchführung dieser Schulungen durch qualifizierte, unabhängige Dritte würde zu einem höchstmöglichen Sicherheitsniveau beitragen.
- Gem. Art. 1, § 45 (3) sind die Informationssicherheitsbeauftragten für den Aufbau und die Aufrechterhaltung des Informationssicherheitsprozesses der Einrichtung zuständig. Sie erstellen ein Informationssicherheitskonzept, welches mindestens die Vorgaben des Bundesamtes nach § 44 Absatz 1 erfüllt.
  - Die Prüfung und Bewertung eines solchen Informationssicherheitskonzeptes durch qualifizierte, unabhängige Dritte, würden hierbei zu einem höchstmöglichen Sicherheitsniveau beitragen.
- Artikel 1 und Artikel 16 sehen zur weiteren Fortentwicklung der Cyber- und IT-Sicherheitsanforderungen die Beteiligung externer Dritter im weiteren Abstimmungsprozess vor. DEKRA bietet insbesondere bzgl. der folgenden Aspekte gerne seine Expertise an:
  - Art. 1, §3, Aufgaben des BSI, (1) Punkt 27: Beschreibung und Veröffentlichung eines Standes der Technik bei sicherheitstechnischen Anforderungen an IT-Produkte, unter Einbeziehung der betroffenen Wirtschaftsverbände.
  - Art. 1, §30, Risikomanagementmaßnahmen besonders wichtiger Einrichtungen und wichtiger Einrichtungen, (9): Vorschlag

branchenspezifischer Sicherheitsstandards zur Gewährleistung der Anforderungen durch besonders wichtige Einrichtungen und ihre Branchenverbände.

- Art. 1, §57, Ermächtigung zum Erlass von Rechtsverordnungen, (1): Anhörung der betroffenen Wirtschaftsverbände zum Verfahren der Erteilung von Sicherheitszertifikaten und Anerkennungen nach § 54 und deren Inhalt.
- Art. 16, §5c, IT-Sicherheit im Anlagen- und Netzbetrieb, (1): Beteiligung der Betreiber von Energieversorgungsnetzen und deren Branchenverbände.

Über die Berücksichtigung o.g. Anregungen im weiteren legislativen Prozess würden wir uns freuen und stehen für weitergehende Gespräche sehr gerne zur Verfügung.

Mit freundlichen Grüßen



Dr. Fabienne Beez  
Leiterin  
DEKRA Konzernrepräsentanz Berlin



Moritz Harich  
Senior Referent  
DEKRA Konzernrepräsentanz Berlin

## **Über DEKRA**

A decorative green arrow graphic pointing to the right, located on the left side of the page.

*Seit fast 100 Jahren arbeitet DEKRA für die Sicherheit: Aus dem 1925 in Berlin gegründeten Deutschen Kraftfahrzeug-Überwachungs-Verein e.V. ist eine der weltweit führenden Expertenorganisationen geworden. Die DEKRA SE ist eine hundertprozentige Tochtergesellschaft des DEKRA e.V. und steuert das operative Geschäft des Konzerns. Im Jahr 2022 hat DEKRA einen Umsatz von fast 3,8 Milliarden Euro erzielt. Knapp 49.000 Mitarbeiterinnen und Mitarbeiter sind in rund 60 Ländern auf fünf Kontinenten im Einsatz. Mit qualifizierten und unabhängigen Expertendienstleistungen arbeiten sie für die Sicherheit im Verkehr, bei der Arbeit und zu Hause. Das Portfolio reicht von Fahrzeugprüfungen und Gutachten über Schadenregulierung, Industrie- und Bauprüfung, Beratungs- und Schulungsleistungen sowie die Prüfung und Zertifizierung von Produkten und Systemen, auch in der digitalen Welt, bis zur Zeitarbeit. Die Vision bis zum 100. Geburtstag im Jahr 2025 lautet: DEKRA wird der globale Partner für eine sichere und nachhaltige Welt. DEKRA gehört schon heute mit dem Platinum-Rating von EcoVadis zu den Top-1-Prozent der nachhaltigen Unternehmen im Ranking.*