Stellungnahme

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

Bundesministerium des Innern
Alt-Moabit 140
10557 Berlin

Dr. Daniel Meltzian
Leiter Referat CI 1 – Grundsatz;
Cyber- und Informationssicherheit

Berlin, 4. Juli 2025

DEKRA Position zum „Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung“
(NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz – NIS2UmsuCG)

Sehr geehrter Herr Dr. Meltzian,
sehr geehrte Damen und Herren,

im Zeitraum 2023 bis 2024 verursachten Cyberangriffe allein für die deutsche Wirtschaft einen Rekordschaden von rund 267 Milliarden Euro. Die Studie des BITKOM[1] zeigt, dass acht von zehn Unternehmen von Datendiebstahl, Spionage oder Sabotage betroffen sind – zwei Drittel der Unternehmen fühlen sich in ihrer Existenz bedroht. Die Bedrohungslage im Cyberraum ist damit so ernst wie nie zuvor.

Mit 100 Jahren Erfahrung und rund 48.000 Mitarbeitenden ist DEKRA eine der weltweit führenden, unabhängigen Prüf- und Expertenorganisationen. Im Hinblick auf Cybersicherheit 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

[1] Angriffe auf die deutsche Wirtschaft nehmen zu | Presseinformation | Bitkom e. V.

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 Cybersicherheit von Produkten und Anwendungen für die Zulieferer globaler Tech-Unternehmen. Als eine der ersten akkreditierten Zertifizierungsstellen in Deutschland bietet DEKRA Cybersicherheitsdienstleistungen für Automobilhersteller an. DEKRA ist auch eine Konformitätsbewertungsstelle (CAB), die aus einer akkreditierten Zertifizierungsstelle (CB) und einer Einrichtung zur Bewertung der Sicherheit von Informationstechnologie (ITSEF) besteht und im Rahmen des EUCC-Programms auf einem hohen Vertrauensniveau arbeitet.

Wir bedanken uns für die Möglichkeit zu einer schriftlichen Stellungnahme im Rahmen der Beteiligung von Fachkreisen und Verbänden zum Referentenentwurf sowie zu der Teilnahme an der Anhörung am 4. Juli 2025 in Berlin.

Nachstehende Anmerkungen sind aus unserer Sicht zentral:

Die nationale Umsetzung der NIS-2 Richtlinie ist eine wichtige Maßnahme zum Schutz der digitalen Infrastrukturen in Deutschland und gerade in der aktuellen herausfordernden geopolitischen Lage unabdingbar. Im Sinne einer europäisch harmonisierten, widerstandsfähigen digitalen Infrastruktur leistet DEKRA einen grundlegenden Beitrag zu einem höchstmöglichen Cybersicherheitsniveau. Damit können wir nachgelagerte Behörden unterstützten und entlasten - indem wir IT-Anwendungen von Unternehmen absichern, fungiert DEKRA als wichtiger Enabler für Innovationen. Im Sinne der Prävention sind auch vorgeschriebene Trainingsmaßnahmen wichtig.
Entscheidend ist dabei, dass die TIC-Branche als unabhängiger Akteur im Rechtsrahmen fest verankert wird.

Vor diesem Hintergrund begrüßt DEKRA insbesondere Artikel 1, § 14, § 52 und § 65, die das Hinzuziehen anerkannter Sachverständiger bzw. qualifizierter, unabhängiger Dritter für die Zertifizierung bzw. für Aufsichts- und Durchsetzungsmaßnahmen vorsehen.

- In § 52 sollte dabei spezifiziert werden, für welche *„bestimmte[n] Produkte und Leistungen“* anerkannte sachverständige Stellen hinzugezogen werden können, bzw. müssen. Als unabhängige dritte Stelle verfügt DEKRA über ein umfassendes Serviceportfolio in den Bereichen Training, Consulting, Auditierung, Product Testing und Zertifizierung. Es kommt in den Dienstleistungsbereichen Automotive, Industrial IoT, Medical Devices, FMCG oder ICT zum Einsatz.

- 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 bereitgestellte oder zur Bereitstellung auf dem Markt vorgesehene informationstechnische Produkte und Systeme untersuchen. Es ~~kann~~ soll sich hierbei der Unterstützung Dritter bedienen, soweit berechtigte Interessen des Herstellers der betroffenen Produkte und Systeme dem nicht entgegenstehen."

- Nach § 53 (Konformitätsbewertung und Konformitätserklärung) kann das Bundesamt für die vom Bundesamt in einer Technischen Richtlinie festgelegten Anforderungen und Vorgaben zulassen, dass ein Hersteller oder Anbieter von IKT-Produkten, IKT-Diensten und IKT-Prozessen, die keine Verbraucherprodukte nach § 55 sind, **sowie eine Person, oder ein IT-Sicherheitsdienstleister** eine Selbstbewertung seiner oder ihrer Konformität vornehmen. *„Der Hersteller oder Anbieter von IKT-Produkten, IKT-Diensten und IKT-Prozessen, die Person oder der IT-Sicherheitsdienstleister kann unter den Voraussetzungen von Satz 1 eine Konformitätserklärung ausstellen, die bestätigt, dass er oder sie die in der Technischen Richtlinie festgelegten Anforderungen erfüllt. Durch die Ausstellung der Konformitätserklärung übernimmt der Hersteller oder Anbieter der IKT-Produkte, IKT-Dienste und IKT-Prozesse, die Person oder der IT-Sicherheitsdienstleister (Aus-steller) die Verantwortung dafür, dass das IKT-Produkt, der IKT-Dienst, der IKT-Prozess, die Person oder die IT-Sicherheitsdienstleistung den in der Technischen Richtlinie festgelegten Anforderungen entspricht."*

  - Grundsätzlich ist es zu begrüßen, dass aufgrund einer Ausweitung der Sektoren, geeignete Maßnahmen ergriffen werden, um die Vielzahl der notwendigen Dienstleistungen in diesem Bereich sicherzustellen. Hier sollte jedoch auf das etablierte System der Konformitätsbewertungsstellen zurückgegriffen werden.

Bei „7. (3)" schlägt DEKRA die folgende Formulierung vor: *„Wird in den Vorgaben nach Absatz 2 festgelegt, dass die Angaben der Konformitätserklärung nur durch eine akkreditierte Konformitätsbewertungsstelle nachgewiesen können, so ~~kann~~ soll das Bundesamt auf Antrag Konformitätsbewertungsstellen, die im Anwendungsbereich dieses Paragraphen tätig werden, eine Befugnis erteilen, 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, § 55 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 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 Verbraucherschutzes 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 trägt zu einem höchstmöglichen Sicherheitsniveau bei.

- 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 trägt zu einem höchstmöglichen Sicherheitsniveau bei.

- 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 und Zertifizierungen durch qualifizierte, unabhängige Dritte tragen zu einem höchstmöglichen Sicherheitsniveau bei.

- 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 Risikomanagementpraktiken 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 trägt zu einem höchstmöglichen Sicherheitsniveau bei.

- Gem. Art. 1, § 45 (3) sind die Informationssicherheitsbeauftragten für den Aufbau und die Aufrechterhaltung des Informationssicherheitsprozesses der Einrichtung zuständig. Sie erstellen ein Informationssicherheitskonzept, das mindestens die Vorgaben des Bundesamtes nach § 44 Absatz 1 erfüllt.

  - Die Prüfung und Bewertung eines solchen Informationssicherheitskonzeptes durch qualifizierte, unabhängige Dritte, trägt zu einem höchstmöglichen Sicherheitsniveau bei. Daher wird die explizite Erwähnung in der Begründung Zu Absatz 3 (S. 177) begrüßt.

- 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, § 56, Ermächtigung zum Erlass von Rechtsverordnungen, (1): Anhörung der betroffenen Wirtschaftsverbände zum Verfahren der Erteilung von Sicherheitszertifikaten und Anerkennungen nach § 54 und deren Inhalt.

- Art. 17, § 5c IT-Sicherheit im Anlagen- und Netzbetrieb, Festlegungskompetenz (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 gerne zur Verfügung.

Mit freundlichen Grüßen

Dr. Fabienne Beez
Leiterin
DEKRA Konzernrepräsentanz Berlin

Marc Krüger
Senior Referent
DEKRA Konzernrepräsentanz Berlin

Über DEKRA

Seit 100 Jahren steht DEKRA für Sicherheit. 1925 mit dem ursprünglichen Ziel gegründet, die Verkehrssicherheit durch Fahrzeugprüfungen zu gewährleisten, hat sich DEKRA zur weltweit größten unabhängigen nicht börsennotierten Sachverständigenorganisation im Bereich Prüfung, Inspektion und Zertifizierung entwickelt. Heute begleitet das Unternehmen als globaler Partner seine Kunden mit umfassenden Dienstleistungen und Lösungen, um Sicherheit und Nachhaltigkeit weiter voranzutreiben – ganz im Sinne des DEKRA Jubiläumsmottos "Securing the Future". Im Jahr 2024 hat DEKRA einen Umsatz von 4,3 Milliarden Euro erzielt. Rund 48.000 Mitarbeitende sind in etwa 60 Ländern auf fünf Kontinenten mit qualifizierten und unabhängigen Expertendienstleistungen im Einsatz. Mit rund 33 Millionen Fahrzeugprüfungen im Jahr 2024 ist DEKRA weltweit führend und trägt zur sicheren und nachhaltigen Transformation des Mobilitätssektors bei. Zum DEKRA Dienstleistungsportfolio gehören dabei u.a. die Bereiche Schadengutachten, Unfallforschung sowie Prüfungen am Gesamtfahrzeug.