Positionspapier

Thema

Cybersecurity – Umsetzung der NIS-II Richtlinie

- Die Maßnahmen der Bundesregierung zur Weiterentwicklung der NIS-2-Gesetzgebung zum Schutz kritischer Infrastrukturen sind notwendig und werden ausdrücklich begrüßt.
- Eine klare Festlegung der Kompetenzen zwischen Akkreditierung und Zertifizierung ist von grundlegender Bedeutung. Bei der Zertifizierung können unabhängige Prüforganisationen einen wesentlichen Beitrag zur Entlastung der Vielzahl der von der NIS-2 Regelung erfassten Unternehmen leisten.
- Dritte, unabhängige Prüforganisationen können bei der Setzung von Branchenstandards unterstützen. DEKRA bietet hier seine Expertise an

WORUM GEHT ES?

- Der Cybersecurity Act aus Juni 2019 (CSA) hat die Agentur der Europäischen Union für Cybersicherheit (ENISA) deutlich gestärkt und einen Rahmen für die Zertifizierung von IKT-Produkten, -Diensten und -Prozessen geschaffen. Bei ENISA werden die technischen Grundlagen für spezifische Zertifizierungssysteme wie EUCC (Common Criteria-based European Cyber Security Certification Scheme) und das EUCS (Cloud Services Certification Scheme) entwickelt.
- Am 15. September 2022 hatte die Europäische Kommission ihren Vorschlag zum Cyber Resilience Act (CRA) veröffentlicht: Weltweit werden die Schäden aufgrund von Cyberattacken (Hardware & Software) auf 5,5 Billionen Euro geschätzt, alle elf Minuten kommt es zu dem Versuch eines Cyberangriffs.
- Der CRA soll bereits bestehende Rechtsvorschriften wie die NIS-1 und -2 Richtlinien oder den Cybersecurity Act ergänzen und die Konsistenz der EU-Gesetzgebung weiter stärken. Hierzu ist die Einteilung in drei Risikogruppen geplant: 1. unkritische Produkte mit digitalen Komponenten (90 Prozent der

Datum Berlin, 03.11.2023
Kontakt Dr. Fabienne Beez
Telefon 030. 986098810
E-Mail fabienne.beez@dekra.com

DEKRA SE
Konzernrepräsentanz Berlin
Behrenstraße 29
D-10117 Berlin
www.dekra.de/presse

Produkte), 2. kritische Produkte mit digitalen Elementen Klasse I sowie 3. hochkritische Produkte mit digitalen Elementen. 10 Prozent der Produkte fallen unter die kritischen Klassen II und III. Hersteller sind nach den Plänen des CRA künftig verpflichtet, über die gesamte Wertschöpfungskette eines Produkts mit digitalen Elementen die Anforderungen des CRA an die Cybersicherheit zu erfüllen. Zudem müssen Hersteller ihre Produkte während des gesamten Lebenszyklus überwachen.

- Die Umsetzung der NIS-1 und NIS-2 Richtlinien sollen die Netzwerk- und Informationssicherheit gewährleisten: „Die NIS-Richtlinie – das erste Cybersicherheitsrecht der EU – ist das erste horizontale Binnenmarktinstrument, das darauf abzielt, die Widerstandsfähigkeit von Netz und Informationssystemen in der Union gegen Cybersicherheitsrisiken zu verbessern.“ Damit sollen explizit kritische Infrastrukturen geschützt werden.
- Das Gesetz zur nationalen Umsetzung „zur Gewährleistung einer hohen Netzwerk- und Informationssicherheit“ (NIS-1-Richtlinie) wurde am 29. Juni 2017 verkündet. NIS-1 möchte eine gemeinsames Sicherheitsniveau, Ressourcenaufbau und Meldepflichten u.a. für kritische Infrastrukturen schaffen. Die NIS-1-Richtlinie umfasst die Sektoren: Energie, Verkehr, Banken, Finanzmarktinfrastrukturen, Trinkwasser, Gesundheitsversorgung und digitale Infrastruktur.
- Die NIS-2-Richtlinie ist am 27. Dezember 2022 in Kraft getreten und muss von Seiten der Nationalstaaten innerhalb von 21 Monaten umgesetzt werden. Mit neuen Einrichtungskategorien soll der Anwendungsbereich voraussichtlich deutlich ausgeweitet werden. Es wird zwischen „besonders wichtigen“ und „wichtigen“ Einrichtungen unterschieden. Nach Schätzungen des Statistischen Bundesamtes werden über 29.000 Unternehmen von der neuen Regelung betroffen sein. Sowohl NIS-1 als auch NIS-2 stehen in Zusammenhang mit den IT-Sicherheitsgesetzen 1.0 und 2.0.
- Die deutsche Transposition der NIS 2 wird mit einer Überarbeitung des sog. BSI-Gesetzes (Bundesamt für Informationssicherheit) einhergehen. Das Bundesministerium des Innern und für Heimat (BMI) hatte am 2. Oktober 2023 ein Gesetzgebungsentwurf veröffentlicht.

DAS IST UNSERE POSITION

- Die deutsche Transposition zur nationalen Implementierung von NIS-2 sollte einen klaren Hinweis auf zu erwartende Akkreditierungskompetenzen liefern und zur Gewährleistung institutioneller Unabhängigkeiten zwischen

Akkreditierung und Zertifizierung unterscheiden. Der derzeitige Entwurf des Bundesinnenministeriums beinhaltet keine eindeutige Rollendefinition der sog. neutralen oder benannten Stellen (vgl. §57). Zur Vermeidung möglicher Mehrfachprüfgen und Nachweispflichten sollten entsprechende Vorgaben gemacht werden.

- §57, Absatz 2 bezieht sich in diesem Zusammenhang auf die Verpflichtung für eine Selbsterklärung zur IT-Sicherheit für Unternehmen im besonderen öffentlichen Interesse (UNBÖFI). Dies kann aus Sicht von DEKRA dazu beitragen, die IT-Sicherheit dieser Unternehmen langfristig zu erhöhen. Hier sollte die Gesetzgebung unabhängige Prüfstellen wie DEKRA bei der Zertifizierung berücksichtigen und die langjährige Expertise – dies auch mit Blick auf die Reichweite und Vielzahl der betroffenen Unternehmen – nutzen.
- Die durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) definierten IT-Sicherheitsanforderungen sollten darüber hinaus durch eine Aktualisierung der Technischen Richtlinien kontinuierlich dem jeweiligen Stand der Technik angepasst werden. Damit kann aktuellen technischen Entwicklungen Rechnung getragen und die Zielsetzung des Sicherheitskennzeichens zu mehr Verbraucherschutz fortlaufend gesichert werden.
- Im Gesetzentwurf wird der Sektor Verkehr inkl. vernetzter Steuerungsanlagen der Kritischen Infrastruktur (KRITIS) zugeordnet (vgl. Anlage 1, Punkt 2). OEMs und Lösungsanbieter betreiben im Rahmen der aktuellen Zulassungsprozesse bereits großen Aufwand (R155/156). Darum ist der Aufbau einer gleichwertigen Prüfinfrastruktur mit ausreichend personellen Ressourcen, z.B. in Prüflaboren, erforderlich. Vor dem Hintergrund des Fachkräftemangels kann hier eine kooperative Herangehensweise zwischen BSI und TIC-Gesellschaften zielführend sein. - Es ist aus Sicht der TIC-Branche vor diesem Hintergrund unerlässlich, dass verpflichtende Audits und sowie Periodisch Technische Untersuchungen (PTI) in die deutsche NIS 2 Transposition einfließen – mit einer gleichzeitigen Kompetenzregelung zwischen BSI und neutralen Stellen.
- Der Gesetzesentwurf klärt die Rollen- und Kompetenzverteilung zwischen BSI und KBA im Hinblick auf UNECE R155/R156 nicht ausreichend. Es ist in diesem Zusammenhang insbesondere zu klären, wer welche Kompetenzen zur Prüfpflicht hat. Nach aktuellem Stand wäre bspw. eine Bewertung von UNECE R155/R156 auf der Basis von ISO 21434 durch das BSI rechtlich nicht möglich, da dem Kraftfahrt-Bundesamt hier die Hoheit obliegt.
- Aus Sicht von DEKRA ist es zwingend erforderlich, Business Continuity Management (BCM) im Rahmen einer unabhängigen Prüfung bei relevanten kritischen Infrastrukturen zu verankern – wie bspw. auf Grundlage einer ISO

22301 Zertifizierung oder einer angelehnten Validierung. So kann ein gesamtheitliches Notfall- und Krisenmanagement der kritischen Infrastruktur einer Organisation über die reine IT hinaus bestätigt werden.

- In §30 im Gesetzesentwurf ist ein umfassender Katalog von Risikomanagementmaßnahmen besonders wichtiger Einrichtungen und wichtiger Einrichtungen aufgeführt. Bei der Erstellung von branchenspezifischen Sicherheitsstandards bietet DEKRA sehr gern seine Expertise an.
- In §38 wird auf die sog. Billigungs-, Überwachungs- und Schulungspflicht für Geschäftsleiter besonders wichtiger Einrichtungen verwiesen. Zertifizierte Nachweise unabhängiger Dritter, die die erfolgreiche Absolvierung dieser Schulungen belegen, sind wichtig und können zur Sicherung von Qualitätsstandards beitragen.
- Der Transpositionsentwurf erweitert die Liste der kritischen Unternehmen signifikant (vgl. Anlage 1 und 2). Aus Sicht von DEKRA könnte in diesem Zusammenhang eine einfachere Lesbarkeit des Gesetzes im Sinne einer praxisfreundlicheren Umsetzung zielführend sein. Dies könnte z.B. durch eine Liste von Ausschlusskriterien für Unternehmen erzielt werden.

Über DEKRA

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.