ZENTRALVERBAND DEUTSCHES BAUGEWERBE ZDB

Stellungnahme zum Referentenentwurf eines NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetzes (NIS2UmsuCG) vom 23.06.2025

Berlin, 04.07.2025
Zentralverband Deutsches Baugewerbes (ZDB)
Hauptabteilung Unternehmensentwicklung
Referat Digitalisierung
afsar@zdb.de
Lobbyregister der Bundesregierung: R005093

Vorbemerkungen

Der Zentralverband Deutsches Baugewerbe (ZDB) ist der größte und älteste Bauverband in Deutschland. Wir vertreten die Interessen von rund 35.000 Bauunternehmen aus Handwerk und Mittelstand, die familien- und inhabergeführt und größtenteils seit Generationen vor Ort tätig sind – im klassischen Hochbau, Straßen- und Tiefbau. Wir sind zudem die starke Stimme des Holzbaus und des Ausbaus. Wir schließen seit 125 Jahren Tarifverträge auf Bundesebene für das Bauhauptgewerbe ab. Wir beschäftigen rund 75 % aller Arbeitnehmerinnen und Arbeitnehmer der deutschen Bauwirtschaft und bilden fast 80 % der Branchenlehrlinge aus. Das Baugewerbe steht für 85 % des Wohnungsbaus und leistet über 60 % des Infrastrukturbaus – insbesondere in den Kommunen vor Ort. Unsere Unternehmen bauen Häuser und Wohnungen, Schulen und Krankenhäuser, Straßen und Schienen für die Menschen in unserem Land. Sie erwirtschaften über 70 Prozent des Branchenumsatzes. Sie sind das Rückgrat der deutschen Bauwirtschaft.

Betroffenheit des Baugewerbes

Die im ZDB organisierten Betriebe sind sowohl klassische Hochbauunternehmen, die Bau- und Instandhaltungsleistungen an Bahnhöfen, Straßen, Umspannwerken, Versorgungsnetzen, Krankenhäusern u. Ä. erbringen, als auch Spezialunternehmen für Verkehrs- und Versorgungsnetze die im Straßen- und Brückenbau (inkl. Sensorik, Verkehrsleittechnik), Leitungs- und Kabeltiefbau (Strom, Gas, Wasser, Fernwärme) und den Bau von Schacht- und Tunnelanlagen (Bahn- und Straßeninfrastruktur) tätig sind. Sie sind somit Auftragnehmer und Teil der Lieferkette von „besonders wichtigen“ und „wichtigen“ Einrichtungen gem. des NIS2UmsuCG.

Allgemeine Anmerkungen

Der Zentralverband des Deutschen Baugewerbes begrüßt das Ziel eines hohen, einheitlichen Cybersicherheitsniveaus.

Der vorliegende Referentenentwurf für das NIS2UmsuCG vom 23.06.2025 weitet den bisher auf KRITIS-Betreiber begrenzten Anwendungsbereich erheblich aus. § 30 Abs. 2 Nr. 4 BSIG-E („Sicherheit der Lieferkette“) verpflichtet künftig alle „besonders wichtigen“ und „wichtigen“ Einrichtungen zur Umsetzung von Maßnahmen zur „Sicherheit der Lieferkette“, einschließlich sicherheitsbezogener Aspekte der Beziehungen zu unmittelbaren Anbietern oder Diensteanbietern.

Diese werden in der Gesetzesbegründung als vertragliche Vorgaben an Zulieferer und Dienstleister zu Risikomanagement, Incident-Response, Patch-Management etc. konkretisiert. Der Referentenentwurf lässt jedoch weder Reichweite noch Tiefe der Anforderungen erkennen.

Somit ist für mittelständische Bauunternehmen, die meist **einmalige oder zeitlich begrenzte Bau- und Instandhaltungsleistungen** an kritischen Infrastrukturen erbringen, **unklar, welchen indirekten Pflichten** sie als Teil der Lieferkette kritischer Betreiber unterliegen, und wer Art und Tiefe dieser Pflichten festlegt (Betreiber, BSI, Ressort-Verordnungen).

Weiterhin nennt § 28 zwar Schwellen (≥ 250 MA bzw. ≥ 50 Mio. € Umsatz für sonstige Dienstleister) für die Einstufung als besonders wichtige und wichtige Einrichtungen. KMU sind von der Lieferketten-Pflichten jedoch nicht ausgenommen. Damit könnte bereits ein Kleinunternehmen, das eine einmalige Sanierungsmaßnahme an einem Bahnhofsdach oder Gleis durchführt, in dieselbe Nachweispflicht geraten wie ein langjähriger IT-Dienstleister.

Auch besteht die Gefahr, dass mittelständige Bauunternehmen über Betreiberverträge mittelbar in Pflicht genommen werden. Auch lässt der Entwurf offen, ob einmalige Bau-, Sanierungs- oder Instandhaltungsprojekte denselben Lieferkettenanforderungen unterliegen wie langfristige IT- oder Logistikdienstleistungen.

Diese Unklarheiten drohen **unverhältnismäßige Audit-, Dokumentations- und Zertifizierungskosten** für kleine und mittlere Bauunternehmen bei minimaler Cyberangriffsfläche zu verursachen.

Besondere Anmerkungen

1. **Reichweite der Lieferkettenpflichten**

   § 30 Abs. 2 Nr. 4 BSIG-E verlangt pauschal die „Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zu unmittelbaren Anbietern oder Diensteanbietern“. Die Gesetzesbegründung nennt beispielsweise vertragsgebundene Vorgaben an Zulieferer (Risiko- & Incident-Management, Patch-Management) und „External Attack Surface (EAS) Scans“. Unbestimmt bleibt dabei, ob diese Pflichten alle Werk- und Dienstverträge – also auch rein bauliche Einmalmaßnahmen – erfassen, welche Risikoschwelle einen EAS-Scan auslöst und ob (Bau-)Unternehmen eigene IT-Prüfpflichten gegenüber Sub-Sub-Unternehmern treffen.

   Damit droht ein **praktisch uferloser Anwendungsbereich ohne klaren Bezug zur tatsächlichen Cyberschnittstelle des Gewerkes**. Für Netzbau-Unternehmen besteht die Gefahr, dass jede Baustelle an einer kritischen Trasse (z. B. Gas-Fernleitung) ein vollständiges IT-Risikomanagement inkl. „External-Attack-Surface-Scans“ auslöst, obwohl vor Ort kein Zugriff auf Betriebs-IT erfolgt.

   Verbesserungsvorschlag

   Eine **Präzisierung des Anwendungsbereichs in Bezug auf Lieferketten-Dienstleister** im Gesetzestext ist erforderlich. Es ist klarzustellen, dass einmalige, bauliche Leistungen nur dann den Lieferkettenpflichten unterliegen, wenn sie (a) unmittelbar betriebsnotwendige IT-Systeme betreffen oder (b) vertraglich eine regelmäßige Interaktion mit kritischen Prozessen vereinbart ist (z. B. durch Einfügung eines § 30 Abs. 2 Nr. 4a BSIG-E). Dieses kann durch einen **neuen § 30 Abs. 2 Nr. 4 a BSIG-E** oder eine Klarstellung in der VO, welche nach § 56 Abs. 5 zu erlassen wäre, erfolgen.

2. **Zuständigkeit/ Steuerung**

   Weiterhin bleibt unklar, wie und durch wen die Lieferkettenpflichten konkretisiert werden. Der Referentenentwurf verweist zwar darauf, dass Details zu den Anforderungen per Verordnung nach § 56 Abs. 5 BSIG-E geregelt werden können, die VO-Ermächtigung ist jedoch nicht ausgefüllt. Parallel kann das BSI jederzeit Nachweise anfordern (§ 61 Abs. 3). **Konkrete Mindeststandards oder Musterklauseln**, die eine Einheitlichkeit gewährleisten, **fehlen**.

   Ohne bundeseinheitliche Vorgaben besteht die **Gefahr heterogener Einzelverträge**, in denen Betreiber kritischer Anlagen die Anforderungen eigenständig festlegen.

Verbesserungsvorschlag

Daher müssen Zuständigkeiten und verbindliche, **einheitliche Mindestanforderungen** für sämtliche Lieferketten-Beziehungen im Gesetzestext festlegt werden. Diese zentralen Leitlinien – etwa **in Form von Musterschutz- und Compliance-Klauseln** – sollen individuelle Betreiber-Verträge ersetzen, um fragmentierte Vertragslandschaften zu vermeiden.

3. Verhältnismäßigkeit/ KMU-Schutz

Der Referentenentwurf schöpft die in Art. 6 und 21 NIS-2 angelegten Spielräume nicht aus. Zwar verlangt § 30 Abs. 1 eine „verhältnismäßige" Umsetzung unter Berücksichtigung von Größe, Risikoexposition und Kosten der Einrichtung. Die Verhältnismäßigkeit in Bezug auf Teile der Lieferkette ist jedoch nicht berücksichtigt.

Dadurch besteht die Gefahr, dass KMUs der Lieferkette Anforderungen erfüllen müssen, die KMU unverhältnismäßig belasten.

Verbesserungsvorschlag

Alle Möglichkeiten der EU-Richtlinie, um KMUs zu entlasten, müssen in der nationalen Gesetzgebung wahrgenommen werden. Dabei muss die Lieferkette unbedingt berücksichtigt werden.

4. Zertifizierungen als De-facto-Pflicht

Die Gesetzesbegründung zu § 30 stellt Zertifikate als „mögliche" Nachweise dar. Zugleich darf das BMI gemäß § 56 Abs. 3 verbindliche Cybersicherheitszertifizierungen für Produkte, Dienste oder Prozesse der Einrichtungen anordnen, wenn „Art und Ausmaß der Risikoexposition" dies rechtfertigen.

Damit entsteht eine **faktische Zertifizierungspflicht**, da für Baubetriebe realistische, Alternativen (z. B. Selbsterklärung) fehlen. Auch könnten Betreiber Zertifikate von der Bau-Lieferkette anfordern, um ihre eigene Nachweispflicht zu erfüllen. Diese faktische Zertifizierungspflicht führt zu **hohen finanziellen Belastungen** mittelständische Bauunternehmen (externe Auditoren, Dokumentation).

Verbesserungsvorschlag

Die **Spielräume** Art. 6 und 21 NIS-2 **müssen** auch in diesem Aspekt **voll ausgenutzt werden**. Dieses kann beispielsweise erreicht werden durch:

- Verzicht auf Zertifizierungspflichten für KMU-Dienstleister.
- Anerkennung branchenspezifischer Selbstbewertungen (DIN 77006-basierte Checklisten).
- Cyber-Schulungen und kostenlose BSI-Tools für OT-Sicherheit.

5. Risikobasierte Eingrenzung für einmalige Bauleistungen

Klassische Baumaßnahmen an Anlagen der kritischen Infrastruktur sind größtenteils einmalig und zeitlich begrenzt. Sie greifen dabei nicht in IT-Systeme der kritischen Anlagen ein. Wird im Rahmen von Baumaßnahmen Sensorik oder Steuerungstechnik eingebracht, besteht eine echte IT-Schnittstelle.

Es besteht die Gefahr, dass überzogene Anforderungen an die Bauunternehmen gestellt werden, ohne dass ein wirkliches Einfallstor für Angriffe auf die Cybersicherheit besteht.

Verbesserungsvorschlag

Daher bedarf es einer **risikobasierten Abstufung der Anforderungen** nach Interaktionshäufigkeit und Kritikalität. **Zwei Risikokategorien** für Bauleistungen können dabei betrachtet werden:

- Physische Arbeiten ohne digitale Einbindung (reiner Straßen-/Brücken-/Leitungsbau): Selbsterklärung nach Musterformular; keine Zertifizierungs- oder Scan-Pflicht.
- Bauleistungen mit OT-Integration (Einbau/Anschluss von Sensorik, SCADA-Kabeln, Ladeinfrastruktur): sektorspezifische Mindestmaßnahmen (z. B. abgesichertes Laptop, Schulung „OT-Hygiene“, Sign-off mit Betreiber).

6. Sonderregelung für öffentlich Betreiber

Gemäß § 28 Abs. 9 BSIG-E bestehen für öffentliche Einrichtungen Sonderregelungen.

Die Nutzung dieser Öffnungsklausel darf nicht dazu führen, dass etwa kommunale Bauhöfe gegenüber privatwirtschaftlichen Bauunternehmen unfaire Wettbewerbsvorteile erhalten.

Verbesserungsvorschlag

Es bedarf der Klärung, ob Bauleistungen für kommunale Bahnhöfe/Kliniken unter dieselben Lieferkettenpflichten fallen wie für private Betreiber.

Die Unternehmen des Baugewerbes tragen durch Verkehrs-, Leitungs- und Brückenbau zur Resilienz kritischer Infrastruktur bei, ohne selbst digitale Kernprozesse zu betreiben. Ein risiko- und laufzeitbasiertes Modell schützt reale Angriffspunkte (OT-Integration), vermeidet aber unverhältnismäßige Zertifizierungs- und Scan-Kosten für rein physische Bauleistungen.

Ohne klaren Zuschnitt der Regelungen des NIS2UmsuCG auf Bau-Einmalleistungen und ohne bundeseinheitliche Mindestvorgaben laufen mittelständische Bauunternehmen Gefahr, in umfangreiche, kostenintensive IT-Sicherheitsaudits hineingezogen zu werden, obwohl ihr **Beitrag zur digitalen Angriffsfläche der kritischen Infrastruktur marginal** ist. Eine **risikobasierte Eingrenzung** (z. B. Befreiung bei < 30 Tagen Vor-Ort-Einsatz oder bei rein physischen Leistungen) und verbindliche KMU-Erleichterungen sind daher zwingend notwendig.

Wir bitten das BMI, die oben dargestellten Klarstellungen und Erleichterungen in das weitere Gesetz- und Verordnungsverfahren aufzunehmen, um eine praxisgerechte, KMU-freundliche und zugleich wirksame Umsetzung der NIS-2-Richtlinie zu gewährleisten.

Der ZDB steht dem BMI und dem BSI gerne für eine **branchenspezifische Arbeitsgruppe** zur Verfügung, um praktikable Leitlinien auszuarbeiten und die Einführung flankierender Awareness-Programme zu unterstützen.