Gesetzesentwurf zur Umsetzung der NIS-2-Richtlinie

Stellungnahme

Berlin, 12.11.2025

Vorbemerkungen

Nach längerem Umsetzungsverzug will die Bundesregierung mit dem NIS-2-Umsetzungsgsetz die europäischen Vorgaben zur Stärkung der Cybersicherheit (RL (EU) 2022/2555) in nationales Recht überführen. Das Ziel eines hohen Schutzniveaus für Netz- und Informationssysteme ist ausdrücklich zu begrüßen, setzt jedoch voraus, dass die Umsetzung verhältnismäßig, praxistauglich und mittelstandsgerecht erfolgt.

Hinter diesem Anpruch bleibt der vorliegende Entwurf zurück. In zentralen Punkt führt er sogar zu einer unangemessenen Übererfüllung der europäischen Vorgaben – obwohl die Bundesregierung sich im Koalitionsvertrag explizit zum Ziel gesetzt hat, sogenanntes „Gold Plating“ künftig auszuschließen.

Zu § 28 Abs. 3: Ausnahmen von „Nebentätigkeiten“

In § 28 Abs. 3 entscheidet sich der Gesetzgeber, solche Einrichtungen vom Anwendungsbereich des Gesetzes auszunehmen, deren in den Anhängen I und II genannten Geschäftstätigkeiten lediglich eine „Nebentätigkeit“ darstellen. Grundsätzlich ist diese Ausnahme zu begrüßen, da sie verhindert, dass untergeordnete oder geringfügige Tätigkeiten eine unverhältnismäßige regulatorische Belastung für Unternehmen nach sich ziehen. Darüber hinaus stellt die im aktuellen Änderungsantrag vorgenommene Ersetzung des Begriffs *„vernachlässigbare Geschäftstätigkeit“* durch *„Nebentätigkeit“* eine sprachliche und systematische Verbesserung gegenüber dem Regierungsentwurf dar.

Allerdings bleibt auch dieser Ausnahmetatbestand rechtlich unbestimmt und führt in der Praxis weiterhin zu erheblicher Unsicherheit. Dies betrifft etwa Verbundgruppen, die ihren angeschlossenen, rechtlich selbstständigen Mitgliedsunternehmen zentrale Online-Verkaufsplattformen bereitstellen. Es bleibt unklar, anhand welcher wirtschaftlichen Kriterien – etwa Umsatzanteil, Transaktionsvolumen oder Gewinnrelevanz – eine Geschäftstätigkeit als *Nebentätigkeit* qualifiziert wird und welche quantitativen Schwellenwerte hierfür gelten sollen.

- **Wir fordern die Gesetzgeber auf, weitere Klarstellung dazu vorzunehmen, inwiefern eine Nebentätigkeit eine qualifizierende Wirkung auf den Ausnahmetatbestand nach § 28 Abs. 3 NIS-2-E entfaltet.**

Zu § 30 Abs. 6: Zertifizierung von IKT-Produkten

§ 30 Abs. 6 verpflichtet Einrichtungen, die im Sinne der Anlagen I und II als wichtige oder besonders wichtige Einrichtungen gelten, dazu, bestimmte IKT-Produkte, -Dienste und -

DER MITTELSTANDSVERBUND – ZGV e.V. · Unter den Linden 17 · 10117 Berlin
Tel.: 0 30 / 59 00 996-63 · Fax: 030 / 59 00 996-17 · E-Mail: info@mittelstandsverbund.de · Internet: www.mittelstandsverbund.de
Bankverbindung: Volksbank Köln Bonn eG · Kto.-Nr.: 1203000010 · BLZ 380 601 86
BIC: GENODED1BRS · IBAN: DE 28 3806 0186 1203 0000 10
Lobbyregister des Deutschen Bundestages: Registernummer R001283
EU-Transparenzregister: 196997510883-76

Prozesse nur dann zu verwenden, wenn diese im Rahmen eines EU-Cybersicherheitszertifizierungsschemata zertifiziert sind.

Leider verpasst es der deutsche Gesetzgeber auch an dieser Stelle, seinen nationalen Umsetzungsspielraum zu nutzen: Die NIS-2-Richtlinie verpflichtet die Mitgliedstaaten nicht dazu, eigenständig Zertifizierungspflichten zu schaffen. Sie sieht lediglich vor, dass bestimmte Produkte durch delegierte Rechtsakte der Europäischen Kommission als zertifizierungspflichtig erklärt werden müssen. Die Entscheidung, diesen Mechanismus auch national einzuführen, führt zu einer Überregulierung über das europäische Schutzniveau hinaus.

Hard- und Software im IKT-Bereich sind in der Regel mit hohen Anschaffungskosten und langen Nutzungszyklen verbunden. Ein nachträglicher Ausschluss nicht-zertifizierter, aber sicherheitstechnisch gleichwertiger Systeme würde Unternehmen erheblichen finanziellen und organisatorischen Belastungen aussetzen – ohne erkennbaren Sicherheitsmehrwert.

- **In diesem Zusammenhang fordern wir den Gesetzgeber dazu auf, auf den von der europäischen Kommission durch die einschlägigen Rechtsverordnungen vergebenen harmonisierten Cybersicherheitsstandard zu vertrauen und von § 30 Abs. 6 NIS-2-E keinen Gebrauch zu machen. Sollte es dennoch zum Einsatz des § 30 Abs. 6 kommen, sollte für bereits gekaufte Soft- und Hardware ein Bestandsschutz gelten.**

Zu § 28 Abs. 2 Nr. 3: wichtige Einrichtungen

Der § 28 des Entwurfs legt den persönlichen Anwendungsbereich des NIS-2-Umsetzungsgesetzes fest. Nach der zugrunde liegenden EU-Richtlinie gilt dieser für Unternehmen, die als mittlere Unternehmen im Sinne der Empfehlung 2003/361/EG der Europäischen Kommission einzustufen sind oder deren Schwellenwerte überschreiten – also für Betriebe mit mehr als 250 Beschäftigten, 50 Mio. Euro Jahresumsatz oder 43 Mio. Euro Bilanzsumme. Der deutsche Entwurf weicht hiervon ab und senkt die Schwellen für „wichtige Einrichtungen“ nach § 28 Abs. 2 Nr. 3 auf 50 Beschäftigte sowie 10 Mio. Euro Umsatz bzw. Bilanzsumme ab.

Damit wird der Anwendungsbereich erheblich ausgeweitet und zahlreiche mittelständische Unternehmen in eine Regulierung einbezogen, die die EU-Richtlinie ausdrücklich nicht an sie adressiert. Dabei ist diese Änderung weder europarechtlich erforderlich noch sachlich begründet. Vielmehr konterkariert sie das Prinzip einer verhältnismäßigen und risikoadäquaten Belastung, wonach Unternehmen mit geringerer Risikoexposition auch weniger belastet werden sollten. Entsprechend stellt dies eine klassische Form der Übererfüllung europäischer Vorgaben („Gold Plating“) dar.

- **Wir fordern den Gesetzgeber daher auf, die Schwellen für wichtige Einrichtungen analog zu § 27 Abs. 1 gem. der Kommissionsempfehlung 2003/361/EG an die Systematik der NIS-2-Richtlinie anzupassen.**