

Presseaussendung

Umsetzung NIS-2-Richtlinie: VOICE warnt vor Bürokratielast und fordert praxisnahe Vorgaben im Referentenentwurf für mehr IT-Sicherheit

Unklare Regeln, unterschätzte Kosten und fehlende Kontrollen gefährden Umsetzbarkeit für Unternehmen

Der aktuelle Referentenentwurf des Bundesministeriums des Innern (BMI) zur Umsetzung der NIS-2-Richtlinie bietet wichtige Chancen für mehr Cybersicherheit, lässt aber an entscheidenden Stellen noch Fragen offen: Kosten werden aus Sicht der Unternehmen unterschätzt, Kontrollmechanismen sind zu schwach und wer wofür verantwortlich ist – besonders bei Kontrolle, Haftung und Umsetzung – bleiben bislang unklar. VOICE Bundesverband der IT-Anwender e.V. fordert daher praxisnahe Vorgaben, eine klare Verantwortungsverteilung zwischen Staat und Wirtschaft sowie realistische Übergangsfristen – etwa für Produktzertifizierungen und technische Umstellungen –, damit Unternehmen die NIS-2-Anforderungen tatsächlich umsetzen können.

Berlin, 7. Juli 2025 – „Cybersicherheit darf kein bürokratisches Hindernis sein, sondern muss für Unternehmen praktikabel bleiben“, sagt Robin Kaufmann, Geschäftsführer von VOICE. „Ob die Unternehmen bei den bisherigen Vorgaben mitziehen können, ist insbesondere angesichts der unrealistischen Kostenannahmen fraglich. Wir brauchen klare, realistische Vorgaben, die vor allem kleine und mittlere Unternehmen nicht überlasten.“

Mit seiner Stellungnahme zum Referentenentwurf für das NIS-2- Umsetzungs- und Cybersicherheitsstärkungsgesetz vom 4. Juli 2025 fordert VOICE daher Konkretisierungen – für mehr Planungssicherheit und weniger Bürokratielast.

Die sechs wichtigsten Forderungen für eine praxistaugliche NIS-2-Umsetzung:

1. Realistische Kostenbewertung: Mehrbelastungen zu niedrig angesetzt

Die im Entwurf genannten Mehrkosten von durchschnittlich 76.000 Euro pro Unternehmen und Jahr sind deutlich zu niedrig angesetzt. Schon mittelständische Unternehmen zahlen oft deutlich mehr – etwa für Sicherheitsdienstleistungen, neue Technologien, Abhängigkeiten von Cloud-Diensten (SaaS) und weitere Regulierungen wie den Cyber Resilience Act. Laut Entwurf haben bisher nur 17 Prozent der Unternehmen ausreichend in Cybersicherheit investiert – das widerspricht der Annahme eines geringen Mehraufwands.

2. Gleiche Haftungsregeln für Staat und Wirtschaft

Privatwirtschaftliche Geschäftsleitungen sind bei Versäumnissen in der Cybersicherheit – etwa fehlenden Schulungen – persönlich haftbar. Die Leitungen von Bundesbehörden gelten hingegen laut NIS-2-Entwurf nicht als „Geschäftsleitung“ und sind somit von dieser Pflicht ausgenommen. Laut Robin Kaufmann sendet diese Asymmetrie ein falsches Signal: „Egal ob privat oder staatlich, Cybersicherheit muss Chefsache sein. Unterschiedliche Haftungsregeln schwächen die Verantwortung im öffentlichen Sektor und gefährden dadurch die digitale Resilienz.“

3. Umsetzbare Vorgaben und Best Practices für KMU

Besonders kleine und mittlere Unternehmen (KMU) sind durch die derzeit unbestimmte Anforderung zu „verhältnismäßigen Maßnahmen“ verunsichert, weil unklar bleibt, welcher konkrete Erfüllungsaufwand tatsächlich auf sie zukommt. Um diese Unsicherheit zu vermeiden, ist aus Sicht von VOICE eine rasche Konkretisierung durch Best Practices – idealerweise im Rahmen des neuen BSI-Grundschutzes –, transparente Referenzstandards (B3S, ENISA-Leitlinien) und eine Harmonisierung mit anderen Regelwerken wie dem Cyber Resilience Act, um Doppelregulierungen zu vermeiden, entscheidend.

4. Regelmäßige Kontrollen für nachhaltige Umsetzung

Die Erfahrung zeigt, dass gesetzliche Vorgaben ohne konsequente Kontrolle oft nicht nachhaltig umgesetzt werden. Die bisherige Nachweispflicht für nur 24 Unternehmen greift zu kurz. VOICE plädiert daher für regelmäßige, risikobasierte Prüfungen, um die Einhaltung der Maßnahmen sicherzustellen und Schäden vorzubeugen.

5. Anerkennung kommunaler Kosten und Verantwortung

Cyberangriffe können auch auf Länder- und Kommunalebene erhebliche Kosten verursachen. Kommunen tragen bereits heute zum Ausbau kritischer Infrastrukturen – etwa beim Glasfaserausbau – bei. Das sollte gesetzlich anerkannt und in Förderungen berücksichtigt werden.

6. Klare Regeln für Schwachstellenmanagement

VOICE fordert transparente Vorgaben zur Prüf- und Kontrollpflicht bei IT-Sicherheitsrisiken. Bleiben Schwachstellen länger im Internet sichtbar, kann dies als fahrlässig gelten. Unklar ist jedoch, wie mit unzureichenden Prüfungen kritischer Einrichtungen umgegangen wird. Zudem müssen konkrete Standards – etwa BSI-Empfehlungen, DIN- oder ISO-Normen – als „Stand der Technik“ definiert werden, um Rechtssicherheit zu schaffen.

Weitere wichtige Forderungen:

- **Technische Umsetzbarkeit:** Eine zentrale Online-Plattform zur Abwicklung der Melde- und Nachweispflichten muss frühzeitig bereitgestellt werden.
- **Marktverzerrungen verhindern:** Verpflichtungen zu zertifizierten Produkten dürfen nicht zu Lock-in-Effekten führen. VOICE fordert klare Übergangsfristen sowie wettbewerbsschützende Maßnahmen gegen Monopolisierung.
- **Haushaltsmittel transparent machen:** Der Entwurf bleibt bei den Ausgaben für Umsetzung und Behörden zu vage. VOICE fordert eine nachvollziehbare Aufschlüsselung, um Angemessenheit und Verhältnismäßigkeit der Mittel bewerten zu können.

Über VOICE

VOICE ist das größte unabhängige Netzwerk von IT- und Digitalentscheider:innen im deutschsprachigen Raum und vertritt exklusiv die Interessen der Anwenderunternehmen. Als Plattform für Austausch, Wissenstransfer und politische Interessenvertretung bringt VOICE über 460 Mitgliedsunternehmen zusammen – von DAX- und MDAX-Konzernen bis hin zu mittelständischen Betrieben. Gemeinsam mit ihren Tochtergesellschaften repräsentieren sie rund 4.000 Unternehmen mit einem geschätzten IT-Budget von über 35 Milliarden Euro. Im Zentrum der Arbeit von VOICE stehen konkrete Best Practices zu Digitalisierungsthemen wie KI, Cloud, Cyber Security und Regulatorik. Als starke Stimme der Anwenderunternehmen bringt VOICE ihre Perspektive in Politik, Verwaltung und gegenüber der IT-Anbieterseite ein – mit dem Ziel digitale Handlungsfähigkeit zu sichern und Wettbewerbsfähigkeit nachhaltig zu stärken.

Fotohinweis

Robin Kaufmann, Geschäftsführer von VOICE

Rückfragehinweis

Lisa Behrens

Kommunikationsspezialistin

lisa.behrens@voice-ev.org

+43 67761001562