WIRTSCHAFTSRAT Deutschland

Letzte Kugel – und wir zielen auf uns selbst

Der aktuelle Regierungsentwurf zur NIS2-Umsetzung gefährdet die Sicherheit des Landes

Wirtschaftsrat der CDU e.V.

Die Stimme der Sozialen Marktwirtschaft

Einleitung

Der **Wirtschaftsrat der CDU e.V.** vertritt die Interessen von mehr als **12.000 Unternehmerinnen und Unternehmern** aus allen Branchen und Regionen Deutschlands.

Innerhalb des Wirtschaftsrates bündelt die **Bundesfachkommission Cybersicherheit (BFK)** die Expertise von über **240 Mitgliedsunternehmen** und Fachverbänden – darunter Technologieführer, KRITIS-Betreiber, mittelständische Spezialanbieter, Beratungsunternehmen und Zertifizierungsstellen.

Mit diesem Papier nehmen wir **Position zum aktuellen Entwurf der Bundesregierung** zur Umsetzung der europäischen **NIS2-Richtlinie**. Der Entwurf verkennt die sicherheitspolitische Realität, **unterminiert staatliche Schutzpflichten** und **verlagert Verantwortung an unklare, nicht kontrollierbare Akteure**.

Zentrale Forderung der EU ist die **Stärkung der Cyberresilienz in kritischen Infrastrukturen und der öffentlichen Verwaltung**. Der vorliegende Gesetzesentwurf **verfehlt dieses Ziel grundlegend** – und das in einer Zeit massiver geopolitischer Spannungen und wachsender hybrider Bedrohungen.

1. Politischer Hintergrund

Die **NIS2-Richtlinie** ist ein sicherheitspolitisches Instrument zur Erhöhung des gemeinsamen Schutzniveaus innerhalb der EU. Sie verlangt von den Mitgliedstaaten eine **verbindliche und kohärente Umsetzung**.

Deutschland jedoch:

- **ignoriert bestehende Schwächen**, wie sie z. B. vom **Bundesrechnungshof** nachdrücklich bemängelt wurden,
- **degradiert unzureichende Sicherheitspraktiken** zur neuen Norm,
- und **zieht sich als Staat in zentralen Bereichen** aus seiner eigenen Verantwortung zurück – **nicht nur auf Länder- und Kommunalebene, sondern nun auch im Bund selbst**.

2. Analyse der Hauptkritikpunkte

<u>IT-Grundschutz nur noch für Ministerien verpflichtend</u>

Der Entwurf verpflichtet **ausschließlich Bundesministerien** zur Anwendung des **BSI-IT-Grundschutz-Kompendiums**. **Nachgelagerte Bundesbehörden – obwohl oftmals KRITIS-relevant – sind ausgenommen.**

Der Staat **verzichtet damit auf ein einheitliches Schutzniveau** für seine eigene Verwaltung und öffnet **kritische Angriffsflächen**, die nicht überprüfbar sind.
Das ist sicherheitspolitisch **fahrlässig** und untergräbt die Vorbildfunktion des Staates.

Nach § 29 des Entwurfs sind nachgelagerte Bundesbehörden auch von der generellen Umsetzung der NIS2-Vorgaben gemäß § 30 ausgenommen.

Damit entzieht sich der Bund nicht **nur spezifischen IT-Sicherheitsstandards (wie dem IT-Grundschutz),** sondern auch seiner **Verpflichtung zur umfassenden Umsetzung** der europäischen NIS2-Richtlinie auf operativer Ebene.

Dies konterkariert das Ziel eines kohärenten, durchgängigen Sicherheitsniveaus in der gesamten Bundesverwaltung – und schwächt die staatliche Resilienz in zentralen Bereichen.

Sicherheitsstandards durch dynamische Bezugnahmen entwertet

Statt klarer gesetzlicher Vorgaben enthält der Entwurf **dynamische Verweise** auf „jeweils geltende Fassungen“ von BSI-Standards.

Dies bedeutet:

- **Sicherheitsstandards können künftig abgesenkt werden**,
- **ohne Beteiligung des Parlaments**,
- **ohne Transparenz**,
- und **ohne demokratische Legitimation**.

Der Staat **entzieht sich selbst der Steuerungshoheit** über seine digitale Sicherheitsarchitektur.

Ein konkretes Beispiel positiver Referenz: Der **C5-Kriterienkatalog** des BSI ist ein **etablierter und praktikabler Sicherheitsstandard** im Cloud-Bereich. Die Bundesregierung sollte dessen **rechtlichen Status formalisieren** und den Katalog als **verbindlichen Beschaffungsstandard** etablieren.

Mindeststandards als Obergrenze statt Untergrenze

Der Entwurf bewertet **Mindestanforderungen als ausreichend – selbst für besonders schutzwürdige Systeme**. Das widerspricht der **aktuellen Bedrohungslage** fundamental.

Was „**gerade noch genügt**“, ist **im Krisenfall nicht tragfähig**. **Mindeststandards müssen die Untergrenze sein, niemals das Ziel.**

Orientierung an der NIS2-Durchführungsverordnung fehlt

Die Durchführungsverordnung (EU) 2024/2690 konkretisiert seit Oktober 2024 die Anforderungen aus der NIS2-Richtlinie – insbesondere für **IT-Dienstleister, Cloudanbieter** und Betreiber digitaler Dienste.

Viele Unternehmen sind bereits in der **konzernweiten Umsetzung dieser Vorgaben aktiv** – mit erheblichen Investitionen in **Risikomanagement, Vorfallsmanagement und Rechtsberatung**.

Es ist daher unerlässlich, dass das **nationale Umsetzungsgesetz diese Verordnung vollumfänglich berücksichtigt**. **Abweichungen führen zu doppelten Aufwänden und regulatorischer Verwirrung** – auf Kosten der Wettbewerbsfähigkeit.

Nationale Zertifizierungspflicht nach § 30 (6) ist abzulehnen

Der Entwurf erlaubt eine **nationale Zertifizierungspflicht für IKT-Produkte, -Dienste und -Prozesse** nach Art. 49 der Verordnung (EU) 2019/881 –
per **Rechtsverordnung**, **ohne parlamentarische Kontrolle**.

Diese **Blanko-Ermächtigung** ist:

- **rechtlich fragwürdig**,
- **wettbewerbspolitisch schädlich**,
- und **verfassungsrechtlich riskant**.

Mit dem **Cyber Resilience Act (Verordnung EU 2024/2847)** bestehen bereits **verbindliche, sektorübergreifende EU-Vorgaben**.

Zusätzliche nationale Anforderungen führen zu einer **Fragmentierung des Binnenmarkts** und **erschweren den Marktzugang deutscher Anbieter**.

3. Sicherheitspolitischer Widerspruch

Deutschland investiert Milliarden in moderne Verteidigung – spricht von **Zeitenwende, Wehrhaftigkeit und Resilienz**.

Doch im digitalen Raum:

- wird **Cybersicherheit zurückgefahren**,
- **staatliche Verantwortung geschwächt**,
- und **Behörden von Sicherheitsvorgaben befreit**.

Das ist kein technisches Defizit – es ist ein **sicherheitspolitischer Kurzschluss**. **Wir bauen Mauern – und lassen die digitale Hintertür offen.**

4. Politische Bewertung

Ein Gesetz, das **zentrale Bundesbehörden von verbindlichen Sicherheitsvorgaben** ausnimmt, untergräbt das **Fundament staatlicher Handlungsfähigkeit**.

Der Staat darf nicht das schwächste Glied in seiner eigenen Sicherheitsarchitektur sein.
Er muss:

- **Vorbild**,
- **Maßstab**,
- und **Schutzgarant** sein.

Der vorliegende Entwurf ist mit dem Ziel der NIS2-Richtlinie **nicht vereinbar** –er gefährdet Deutschlands **digitale Souveränität**, **Sicherheit** und **Resilienz**.

5. Empfehlungen der Bundesfachkommission Cybersicherheit

- **Verbindlicher IT-Grundschutz für alle Bundesbehörden – ohne Ausnahmen**. Dies gilt insbesondere für das ITZBund sowie alle Behörden mit konsolidierten oder KRITIS-nahen Aufgaben.

- **Streichung der dynamischen Verweise** auf „jeweils geltende Fassungen“ zugunsten gesetzlich fixierter Sicherheitsstandards.

- **Verpflichtung zur Umsetzung über das Mindeststandardniveau hinaus** bei sicherheitsrelevanten Aufgaben und Infrastrukturen. Den rechtlichen Status und die Anwendbarkeit des **bestehenden C5 Kriterienkatalogs** des BSI für Cloud-Anbieter verbindlich umsetzen.

- **Rechtsverbindliche Weisungs- und Durchsetzungskompetenz** des Bundesamtes für Sicherheit in der Informationstechnik (BSI) gegenüber sämtlichen Bundesbehörden.

- **Einführung einer regelmäßigen, öffentlich zugänglichen Berichtspflicht** über den Umsetzungsstand der Informationssicherheit in allen Bundesbehörden.

- **Verankerung der Vorbildfunktion der öffentlichen Hand** im Bereich Cybersicherheit im Gesetz. Ausbau digitaler Infrastrukturen investieren. Dazu müssen deutlich beschleunigte Planungs- und Genehmigungsprozesse auf allen Ebenen (EU, Bund und Ländern) sichergestellt werden.

- **Schnellere Planungs- und Genehmigungsprozesse** für digitale Infrastrukturen auf EU-, Bundes- und Landesebene.

- **Streichung der Ausnahmeregelung in § 29,** wonach nachgelagerte Bundesbehörden von der Umsetzung der NIS2-Vorgaben gemäß § 30 befreit werden. Für ein flächendeckend hohes Schutzniveau müssen auch diese Behörden uneingeschränkt in die Umsetzungspflichten einbezogen werden.

Fazit:

Deutschland steht vor einer sicherheitspolitischen Wegscheide. Cybersicherheit ist keine Option, sondern Voraussetzung für staatliches Handeln im 21. Jahrhundert.

Der vorliegende **Entwurf verfehlt dieses Ziel**. Die Bundesfachkommission fordert eine grundlegende Überarbeitung – im Interesse der digitalen Souveränität, des Wirtschaftsstandorts Deutschland und der Sicherheitslage im gesamten europäischen Raum.

Die Umsetzung der NIS2-Richtlinie entscheidet darüber, **ob wir Cybersicherheit gestalten – oder ihre Erosion gesetzlich legitimieren**.

Ein Staat, der sich über § 29 selbst von zentralen Umsetzungsanforderungen entbindet, setzt ein **fatales Signal – sowohl gegenüber der Wirtschaft als auch gegenüber europäischen Partnern.**

Cybersicherheit darf nicht an Verwaltungsgrenzen enden. Sie muss kohärent, durchgängig und rechtlich verbindlich gestaltet sein – auf allen staatlichen Ebenen.

Der Staat muss **Leuchtturm sein – nicht Schattenwurf**.