Sicherheit ohne Wachstumsbremse: Die NIS-2-Richtlinie praxistauglich umsetzen

Die deutsche Elektro- und Digitalindustrie trägt maßgeblich zur Sicherheit und Funktionsfähigkeit unserer modernen Gesellschaft bei. Sie entwickelt, liefert und betreibt Komponenten und Systeme, die essenziell für kritische Infrastrukturen sind. Ihre Produkte sind das Rückgrat einer digital vernetzten Wirtschaft und zentral für einen cyberresilienten Wirtschaftsstandort. Unsere Branche ist somit kein reiner Regelungsadressat, sondern ein strategischer Partner bei der Stärkung der Cyberresilienz. Ihre Perspektive muss strukturell in den deutschen Umsetzungsprozess der NIS-2-Richtlinie (Richtlinie (EU) 2022/2555) integriert werden – nicht nur durch formale Anhörungen, sondern durch substanzielle Beteiligung bei der Ausgestaltung von Definitionen, Schwellenwerten, Meldepflichten und technischen Anforderungen.

Eine gut gemachte, kohärente und praxisnahe Umsetzung der NIS-2-Richtlinie ist von entscheidender Bedeutung. Sie ist ein zentraler Baustein für die Stärkung der Cybersicherheit in Europa. Bei der nun anstehenden Umsetzung der Richtlinie in Deutschland sollte auf eine **verhältnismäßige, bürokratiearme und praxisnahe Ausgestaltung des Gesetzes** geachtet werden. Unternehmen brauchen klare Leitlinien und praxisorientierte Unterstützung, um die neuen Anforderungen effizient erfüllen zu können.

Grundsätzlich muss EU-weite Einheitlichkeit das oberste Prinzip bei der nationalen Umsetzung sein. Viele unserer Unternehmen sind mindestens europäisch, wenn nicht international tätig. Jegliche Abweichung in den einzelstaatlichen Umsetzungen hat unnötige Mehraufwände zur Konsequenz. Regulatorische Diskrepanzen erfordern Anpassungen, die Ressourcen binden und die deutsche Wirtschaftskraft hemmen. **Eine europaweit einheitliche und konsistente Umsetzung der NIS-2-Richtlinie ist essenziell.**

Der ZVEI steht bereit, die neue Bundesregierung bei der Umsetzung der NIS-2-Richtlinie zu begleiten und sich aktiv bei der Erarbeitung eines guten und effektiven Umsetzungsgesetzes einzubringen. Für eine erfolgreiche Umsetzung der NIS-2-Richtlinie in Deutschland sind aus Sicht des ZVEI folgende Aspekte essenziell:

- **Länderübergreifend einheitliche Umsetzung der NIS-2-Richtlinie:** Keine zusätzlichen nationalen Anforderungen („Gold Plating“).
- **Zentrale EU-weite Meldeplattform:** Bürokratieabbau und Entlastung durch eine zentrale Meldeplattform für Cybersicherheitsvorfälle und aktiv ausgenutzte Schwachstellen auf EU-Ebene.
- **Klar definierter Anwendungsbereich:** Eindeutige und einheitliche Kriterien für die Einstufung von Unternehmen, um Rechtsunsicherheit zu vermeiden.
- **Strukturiere Einbindung relevanter Expertise**: Die Einbindung von Wirtschaftsverbänden, KRITIS-Betreibern und Wissenschaft, bei der Definition von KRITIS-Dienstleistungen und der Festlegung erheblicher Sicherheitsvorfälle ist zentral für eine praxisnahe und fachlich fundierte Ausgestaltung.
- **Keine Zertifizierungspflicht nach § 30 (6):** Weitreichende Zertifizierungspflichten ohne parlamentarische Kontrolle schwächen den Binnenmarkt und die Wettbewerbsfähigkeit Deutschlands. Von einer diesbezüglichen Vorgabe sollte abgesehen werden.
- **Orientierung an der NIS-2-Durchführungsverordnung:** Die nationale Umsetzung sollte sich eng an der EU-Verordnung (EU) 2024/2690 zur Konkretisierung der technischen und methodischen Anforderungen der Risikomanagementmaßnahmen und zur Präzisierung der Kriterien eines erheblichen Sicherheitsvorfalls orientieren.

- **Konkrete Vorgaben für die Cybersicherheit in der Lieferkette**: Entwicklung einer standardisierten Toolbox zur Stärkung der Cybersicherheit in Lieferketten.

- **Anerkennung etablierter Sicherheitsmaßnahmen:** Vorhandene Zertifizierungen (z. B. ISO 27001) anerkennen, um Bürokratie abzubauen und doppelte Auflagen zu vermeiden.

- **Transparenter Prüfprozess für kritische Komponenten:** Klare Prüfkriterien und Bestandschutz für kritische Komponenten.

- **Förderung qualifizierter Vertrauensdienste im nationalen Recht verankern**: Die NIS2 Richtlinie gibt vor, dass EU-Mitgliedsstaaten in wesentlichen und wichtigen Einrichtungen den Einsatz qualifizierter Vertrauensdienste fördern sollen. Dieser Aspekt sollte im nationalen Recht auch nachvollzogen werden.

1 Länderübergreifend einheitliche Umsetzung der NIS-2-Richtlinie

Im Kontext ihres Arbeitsprogrammes 2025 stellt die EU-Kommission klar, dass sog. „Gold Plating“ – die Erweiterung des Regulierungsrahmens von EU-Richtlinien bei der Umsetzung in nationales Recht – zu einer Fragmentierung des Binnenmarktes führt und eine zusätzliche Belastung darstellt[1]. Defizite in der Umsetzung hemmen Wohlstand und Wettbewerbsfähigkeit und haben zu Folge, dass Menschen und Unternehmen nicht in vollem Umfang von den Vorteilen der EU-Politik profitieren. Dies gilt genauso für die deutsche Umsetzung der NIS-2-Richtlinie.

Konsistenz und Einheitlichkeit sind essenziell, um Verzerrungen innerhalb des europäischen Binnenmarktes zu vermeiden. Die deutsche Umsetzung der NIS-2-Richtlinie sollte sich ausschließlich an der europäischen Vorgabe orientieren, um einheitliche Rahmenbedingungen sicherzustellen. Eine **eins-zu-eins-Umsetzung der EU-Richtlinie** ohne zusätzliche nationale Anforderungen ist entscheidend.

Unternehmen der Elektro- und Digitalindustrie agieren grenzüberschreitend und sind in internationale Wertschöpfungsketten eingebunden. Umso mehr sind sie europaweit auf eine konsistente Regulierung angewiesen. Abweichungen von den europäischen Vorgaben führen zu zusätzlichen Kosten und administrativen Hürden und haben unter Umständen zu Folge, dass Unternehmen ihre Strukturen und Prozesse in jedem Mitgliedstaat individuell anpassen müssen. Dies bindet Ressourcen, die besser in den tatsächlichen Schutz vor Cyberbedrohungen investiert wären.

Eine einheitliche Umsetzung hingegen schafft Planungssicherheit, reduziert administrative Hürden und gewährleistet einen effizienten und resilienten Wirtschaftsstandort in Deutschland und Europa. Die deutsche Bundesregierung sollte sich daher aktiv dafür einsetzen, dass die Umsetzung der NIS-2-Richtlinie europaweit so einheitlich wie möglich erfolgt und nicht über die Vorgaben der Richtlinie hinausgehen.

2 Zentrale EU-weite Meldeplattform

Mit Artikel 23 Absatz 4 der NIS-2-Richtlinie werden Einrichtungen dazu verpflichtet, erhebliche Sicherheitsvorfälle unverzüglich an das zuständige *Computer Security Incident Response Team* (CSIRT) des jeweiligen Mitgliedstaats zu melden. In Deutschland wird diese Funktion das Bundesamt für Sicherheit in der Informationstechnik (BSI) erfüllen und dafür eine zentrale Melde- und Registrierungsplattform bereitstellen.

Ein solches, nationalstaatlich fragmentiertes, Meldesystem stellt international agierende Unternehmen vor große Herausforderungen. Die Kontrolle und der Betrieb ihrer informationstechnischen Systeme basiert oft auf komplexen Strukturen und unterliegt mehreren nationalen Ordnungsrahmen innerhalb der EU. Häufig müssen Unternehmen im Kontext eines erheblichen Sicherheitsvorfalls zunächst dessen Ausmaß definieren, bevor sie ihn einem Mitgliedstaat zuordnen können. So kann die Frist für die Meldepflicht bereits abgelaufen sein, bevor klar ist, bei welchem CSIRT Meldung zu erstatten ist.

Um unnötige Bürokratie zu vermeiden und den Maßnahmenkatalog von Unternehmen im Krisenfall zu simplifizieren, sollte sich Deutschland für die Möglichkeit einsetzen, erhebliche Sicherheitsvorfälle unter der NIS-2-Richtlinie auch an das unter der Verordnung (EU) 2024/2847 – dem Cyber Resilience Act – einzurichtende *Single Reporting Portal* melden zu können. Dies würde sicherstellen, dass betroffene Unternehmen nicht mit unterschiedlichen nationalen Meldepflichten konfrontiert sind und dieselben Vorfälle mehrfach melden müssen. Insbesondere international tätigen Unternehmen würde eine solche Harmonisierung Erleichterungen verschaffen und zu einer effizienteren Koordination zwischen den EU-Mitgliedstaaten beitragen. Gleichzeitig würden nationale Behörden entlastet werden. Eine **zentrale, EU-weite Meldeplattform für Cybersicherheitsvorfälle und aktiv ausgenutzte Schwachstellen** kann zusätzlich zu dem CSIRT-Netzwerk maßgeblich zu Simplifizierung und Bürokratieabbau beitragen, ohne das antizipierte Cybersicherheitsniveau innerhalb der EU zu senken.

[1] EU Kommission (2025): *A simpler and faster Europe: Communication on implementation and simplification*.

3 Klar definierter Anwendungsbereich

Mit Artikel 3 der NIS-2-Richtlinie werden betroffene Unternehmen als „wesentliche“ oder „wichtige Einrichtungen“ eingestuft. Diese Klassifizierung von Unternehmen im Anwendungsbereich des § 28 BSIG-Neu ist nicht eindeutig. Der Anwendungsbereich ist in Teilen missverständlich formuliert und lässt Raum für Interpretation. Insbesondere für Unternehmen mit komplexen Strukturen und vielfältigen Geschäftsfeldern war nicht eindeutig, welcher Kategorie sie zuzuordnen sind und welche Verpflichtungen daraus resultieren. Dies erschwerte die Selbstklassifizierung und erhöhte das Risiko von Fehleinschätzungen.

§ 28 Abs. 3 BSIG-Neu verlangt aktuell, alle Geschäftstätigkeiten eines Unternehmens zu berücksichtigen und nur solche auszunehmen, die im Hinblick auf die gesamte Geschäftstätigkeit vernachlässigbar sind. Das weicht deutlich von der bisherigen Praxis ab, die nur den relevanten Umsatzanteil im NIS-2-Sektor (nach NACE-Klassifikation) einbezieht. Unternehmen brauchen hier eine klare Definition, was als „vernachlässigbare“ oder „geringfügige Nebentätigkeit“ gilt

Grundsätzlich braucht es klare, einheitliche und praxistaugliche Kriterien für die Einstufung betroffener Unternehmen. Ein eindeutig definierter Anwendungsbereich des deutschen Umsetzungsgesetzes muss sicherstellen, dass Unternehmen ihre Verpflichtungen nachvollziehen können und unnötige Rechtsunsicherheiten vermieden werden. Regelungen müssen so gestaltet sein, dass Unternehmen frühzeitig Planungssicherheit haben.

In dieser Hinsicht nimmt Kroatien eine Vorbildfunktion ein. Der EU-Mitgliedstaat hat die NIS-2-Richtlinie bereits im Februar 2024 in seinen nationalen Ordnungsrahmen überführt. Um den dortigen Unternehmen frühzeitig Planungs- und Rechtssicherheit zu verschaffen, waren die zuständigen Behörden der jeweiligen Sektoren angewiesen, Unternehmen im Anwendungsbereich über die sie betreffende Einschlägigkeit der Regulierung zu benachrichtigen. Ein solches Vorgehen wäre auch in Deutschland wünschenswert und wäre eine maßgebliche Hilfe für die hier ansässigen Unternehmen.

4 Strukturierte Einbindung relevanter Expertise

Im aktuellen Entwurf wurde die in früheren Entwürfen vorgesehene Beteiligung von Wirtschaftsverbänden, KRITIS-Betreibern, und der Wissenschaft bei der Definition von KRITIS-Dienstleistungen (§ 56 Abs. 4) sowie bei der Festlegung erheblicher Sicherheitsvorfälle (§ 56 Abs. 5) ersatzlos gestrichen. Diese Beteiligungsrechte hätten eine sachgerechte und praxisnahe Ausgestaltung der jeweiligen Regelungsinhalte unterstützt. Es ist bedauerlich, dass diese Möglichkeit zur strukturierten Einbindung relevanter Expertise nicht weiterverfolgt wurde. Eine **gesetzlich verankerte Konsultation zentraler Stakeholder** würde sowohl zur fachlichen Qualität als auch zur Akzeptanz der Regelungen beitragen.

Ferner fehlt in der Auflistung das Bundesministerium für Digitales und Staatsmodernisierung. Im Sinne der Kohärenz plädieren wir dafür, dass Bundesministerium für Digitales und Staatsmodernisierung ebenfalls aufzuführen, um die Bedeutung der ebenenübergreifenden Digitalisierung und Staatsmodernisierung beim Erlass von Rechtsverordnungen zu berücksichtigen.

5 Keine Zertifizierungspflicht nach § 30 (6)

§ 30 Abs. 6 BSIG-Neu sieht vor, dass besonders wichtige und wichtige Einrichtungen bestimmte IKT-Produkte, -Dienste und -Prozesse nur verwenden dürfen, wenn diese über eine Cybersicherheitszertifizierung nach europäischen Schemata gemäß Artikel 49 der Verordnung (EU) 2019/881 verfügen. § 56 Absatz 3 ermächtigt das Bundesministerium des Innern zudem, per Rechtsverordnung festzulegen, welche Produkte, Dienste und Prozesse dieser Pflicht unterfallen.

Diese weitreichende Blanko-Ermächtigung ist problematisch: Sie ermöglicht eine nachträgliche erhebliche Ausweitung der Anforderungen ohne parlamentarische Kontrolle und läuft damit am Deutschen Bundestag als Gesetzgeber vorbei.

Darüber hinaus besteht für eine nationale Regelung dieser Art keine Notwendigkeit mehr. Mit der Verordnung (EU) 2024/2847 – dem Cyber Resilience Act (CRA) – werden auf EU-Ebene einheitliche und

verbindliche, grundlegende Cybersicherheitsanforderungen an die Eigenschaften und das Schwachstellenmanagement von Produkten mit digitalen Elementen eingeführt und sektorübergreifend harmonisiert. Nationale Zusatzanforderungen würden vor diesem Hintergrund den Binnenmarkt fragmentieren und die Wettbewerbsfähigkeit deutscher Unternehmen schwächen.

Wir schlagen daher vor, von einer „Aktivierung“ dieser Regelung gem. **§ 30 Absatz 6 in Verbindung mit § 56 Absatz 3 abzusehen und keine zusätzlichen nationalen Zertifizierungspflichten jenseits der europäischen Vorgaben einzuführen**.

6 Orientierung an der NIS-2-Durchführungsverordnung

Die NIS-2-Richtlinie wird seit Oktober 2024 durch die Durchführungsverordnung (EU) 2024/2690 konkretisiert. Diese legt technische und organisatorische Anforderungen an das Risikomanagement, sowie die Kriterien eines erheblichen Sicherheitsvorfalls, für Unternehmen im Bereich der digitalen Infrastruktur und Anbieter digitaler Dienste fest. Zahlreiche Industrieunternehmen haben Ihre IT-Services an eine konzerninterne, rechtlich selbständige IT-Gesellschaft ausgelagert. Andere erbringen als Muttergesellschaft IT-Services für sich und für verbundene Unternehmen. Soweit diese IT-Services Cloud-Computing-Dienste oder Rechenzentrumsdienste umfassen, sind die Unternehmen Adressat der NIS2-Durchführungsverordnung 2024/2690.

Zum Zeitpunkt des Bruchs der deutschen Regierungskoalition waren viele Unternehmen demnach bereits intensiv mit der Implementierung der NIS-2-Vorgaben beschäftigt und investierten Zeit und Ressourcen in die diesbezügliche Rechts- und Umsetzungsberatung. Als jüngstes rechtsgültiges Dokument erfuhr die Durchführungsverordnung 2024/2690 große Beachtung und sollte bei der nun anstehenden Umsetzung der Richtlinie in Deutschland unbedingt Beachtung finden. **Das Umsetzungsgesetz sollte in seinen Anforderungen an der Durchführungsverordnung ausgerichtet werden**.

7 Konkrete Vorgaben für die Cybersicherheit in der Lieferkette

Ein elementarer Aspekt der NIS-2-Richtlinie ist die Stärkung der Cybersicherheit entlang von Lieferketten. Betroffene Einrichtungen werden u.a. dazu verpflichtet, verhältnismäßige technische und organisatorische Maßnahmen für die Sicherheit ihrer Lieferkette umzusetzen und werden dazu angehalten, diese Maßnahmen in die vertraglichen Vereinbarungen mit ihren direkten Lieferanten und Diensteanbietern einzubeziehen.

Mit Erwägungsgrund 59 der Richtlinie werden die EU-Mitgliedstaaten explizit dazu aufgefordert, bewährte Verfahren für die Sicherung von Lieferketten zu fördern und Synergien zu schaffen. Ein vielversprechender Ansatz wäre die **Entwicklung einer standardisierten Toolbox gemeinsam mit Industrie und Verbänden, die Unternehmen eine strukturierte Herangehensweise an die Cybersicherheitsanforderungen ihrer Lieferkette bietet**. Diese Toolbox könnte Leitlinien, Vorlagen für Verträge sowie Bewertungskriterien für die Sicherheit von Lieferanten enthalten.

Eine besondere Relevanz hat in diesem Kontext die Schnittstelle zwischen der NIS-2-Richtlinie und dem Cyber Resilience Act (CRA). Der CRA legt verbindliche Cybersicherheitsanforderungen für Produkte mit digitalen Elementen fest. Es ist daher essenziell zu klären, ob die Konformität eines Produkts mit den CRA-Anforderungen automatisch ausreicht, um auch die NIS-2-Vorgaben für die Lieferkettensicherheit auf Produktebene zu erfüllen, oder ob zusätzliche Maßnahmen erforderlich sind.

Eine gut durchdachte Toolbox würde insbesondere kleinen und mittelständischen Unternehmen (KMU) helfen, indem sie praktikable Lösungen zur Umsetzung der komplexen regulatorischen Anforderungen bereitstellt. Damit könnten unnötige Mehrbelastungen vermieden und gleichzeitig ein hohes Sicherheitsniveau entlang der gesamten Lieferkette sichergestellt werden.

8 Anerkennung etablierter Sicherheitsmaßnahmen

Unternehmen der Elektro- und Digitalindustrie investieren seit Jahren in robuste Cybersicherheitsmaßnahmen und orientieren sich dabei an international anerkannten Standards wie der ISO/IEC 27000-Reihe.

Etablierte Informationssicherheitsmanagementsysteme (ISMS) mit ISO27001-Zertifizierung gewährleisten ein strukturiertes und wirksames Risikomanagement und erfüllen bereits zentrale Anforderungen der NIS-2-Richtlinie.

Damit die Umsetzung der Richtlinie effizient, praxisnah und gegenüber anderen EU-Staaten nichtdiskriminierend erfolgt, **sollten bestehende und nachgewiesene Sicherheitsmaßnahmen im deutschen Recht gewürdigt werden**. Dem entsprechend wären die geleisteten Investitionen und das Engagement von Unternehmen, die bereits eine Zertifizierung nach ISO/IEC 27001 besitzen, anzuerkennen.

In Folge sollte das BSI die Risikomanagementmaßnahmen aus Art. 21 der NIS-2-Richtlinie den Anforderungen der ISO/IEC 27001 gegenüberstellen und sicherstellen, dass Unternehmen mit entsprechender Zertifizierung nur für das daraus entstehende Delta Umsetzungsnachweise erbringen müssen. Die Anforderungen der NIS-2-Richtlinie werden durch eine ISO/IEC 27001-Zertifizierung ausreichend abgedeckt, wenn der Anwendungsbereich des ISMS auf das gesamte Unternehmen festgeschrieben wird und vereinzelte „Anleitungen“ aus ISO/IEC 27002 für verbindlich erklärt werden.

9 Transparenter und partizipativer Prüfprozess für den Einsatz kritischer Komponenten

Der neue Entwurf des NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz legt weiterhin strengere Anforderungen an den Einsatz kritischer Komponenten in IT- und OT-Systemen fest

Um wirtschaftliche und technologische Nachteile für Hersteller und Integratoren zu vermeiden, ist ein **transparenter und partizipativer Prüfprozess,** unter Einbeziehung von Industrie, Verbänden und unabhängiger Expertise, erforderlich. Regulatorische Entscheidungen sollten auf klar nachvollziehbaren technischen Kriterien basieren und keine unnötigen Einschränkungen für Unternehmen mit sich bringen. Eine enge Abstimmung mit der Wirtschaft ist notwendig, um sowohl ein hohes Maß an Cybersicherheit als auch die wirtschaftliche Wettbewerbsfähigkeit sicherzustellen.

Es ist essenziell, dass bereits eingesetzte Komponenten, die sich in der Praxis bewährt haben, nur in absoluten Ausnahmefällen nachträglich verboten werden, sofern keine anderen geeigneten milderen Maßnahmen greifen. Wir begrüßen daher, dass die Untersagung bereits eingebauter kritischer Komponenten im BMI auch weiterhin im Einvernehmen mit dem zuständigen Ressort erfolgen soll. Ein **Bestandschutz für bereits eingebaute kritische Komponenten** muss gewährleistet sein, um Investitionssicherheit zu schaffen und unnötige Kosten durch nachträgliche Austauschpflichten zu vermeiden. Das gilt insbesondere für Komponenten, die bereits mit hohem Zeit- und Kostenaufwand erfolgreich zertifiziert wurden, da deren technische Sicherheit somit als bewiesen gelten kann. Unternehmen, die in den vergangenen Jahren erhebliche Mittel in ihre IT- und OT-Infrastrukturen investiert haben, dürfen nicht durch regulatorische Änderungen vor unzumutbare Herausforderungen gestellt werden.

10 Förderung qualifizierter Vertrauensdienste im nationalen Recht verankern

Artikel 24 Absatz 1 der NIS-2-Richtlinie verpflichtet die Mitgliedstaaten, den Einsatz qualifizierter Vertrauensdiensteanbieter in wesentlichen und wichtigen Einrichtungen zu fördern. Dieser Auftrag sollte im deutschen Umsetzungsgesetz ausdrücklich nachvollzogen werden, um Rechtssicherheit zu gewährleisten und den Einsatz vertrauenswürdiger digitaler Dienste gezielt zu unterstützen. Der **Einsatz qualifizierter Vertrauensdienste** erhöht nachweislich die IT-Sicherheit. Sie bieten geprüfte, manipulationssichere Verfahren zur Identifizierung, Signatur und Authentifizierung.

Zudem sollte das nationale Umsetzungsgesetz diesbezüglich Bezug nehmen auf die aktualisierte Verordnung (EU) 2024/1183 (eIDAS 2.0). Damit wird der europäische Rahmen für eine digitale Identität gestärkt, der auf einheitliche und interoperable qualifizierte Vertrauensdiensteanbieter setzt und deren Nutzung in der gesamten Union erleichtert.

Kontakt
Lennard Kreißl • Manager Cybersicherheit • Abteilung Digital- und Innovationspolitik • Bereich Digitalisierung & Recht
Tel.: +49 30 300141 582 • Mobil: +49 162 2664 941 • E-Mail: lennard.keissl@zvei.org

ZVEI e. V. • Verband der Elektro- und Digitalindustrie • Charlottenstr. 35/36 • 10117 Berlin
Lobbyregisternr.: R002101 • EU Transparenzregister ID: 94770746469-09 • www.zvei.org