IMPULSPAPIER

Leitprinzipien für BVMW-Mitgliedsunternehmen zur Umsetzung von NIS 2 und Cyber Resilience Act (CRA)

EIN IMPULSPAPIER DER KOMMISSION INTERNET UND DIGITALES

Einleitung

Cyberangriffe, Erpressung, Sabotage und Lieferkettenmanipulationen sind längst keine Ausnahmefälle mehr, sondern reale Geschäftsrisiken für Unternehmen jeder Größe. Mit der europäischen NIS2-Richtlinie und dem Cyber Resilience Act verschärft die Europäische Union die Anforderungen an Cybersicherheit, Governance und Produktsicherheit deutlich.

Die NIS-2-Richtlinie wurde in Deutschland insbesondere durch das NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG) sowie Änderungen des BSI-Gesetzes und weiterer Fachgesetze umgesetzt. Die konkreten Pflichten für Unternehmen ergeben sich aus diesen nationalen Regelungen. Der Cyber Resilience Act ist eine EU-Verordnung. Er gilt nach seinem Inkrafttreten unmittelbar in allen Mitgliedstaaten, sieht jedoch Übergangsfristen vor, innerhalb derer die betroffenen Unternehmen ihre Produkte und Prozesse anpassen müssen.

Während NIS-2 insbesondere Betreiber wesentlicher und wichtiger Einrichtungen adressiert, betrifft der Cyber Resilience Act perspektivisch nahezu alle Hersteller und Anbieter digitaler Produkte mit Datenverbindungen. Für viele mittelständische Unternehmen bedeutet dies: neue Pflichten, erweiterte Haftungsrisiken und steigende Anforderungen an Organisation, Dokumentation und technische Schutzmaßnahmen.

Dieses Impulspapier richtet sich an die Mitgliedsunternehmen des BVMW und bietet Orientierung, wie die regulatorischen Anforderungen systematisch, verhältnismäßig und strategisch umgesetzt werden können. Es versteht NIS 2 und CRA nicht als isolierte Compliance-Themen, sondern als Bestandteil eines integrierten Chancen- und Risikomanagements, wie es im gleichnamigen Impulspapier der Kommission beschrieben ist. Ziel ist es, Geschäftsführern und Entscheidern einen strukturierten Rahmen zu geben, um regulatorische Anforderungen in nachhaltige Sicherheits- und Resilienzstrategien zu überführen. Es handelt sich nicht um eine vollständige Darstellung aller rechtlichen Pflichten, sondern um eine strategische Einordnung und erste Orientierung für Mitgliedsunternehmen.

Teil 1: Leitprinzipien und Handlungsempfehlungen

Cybersicherheit ist Geschäftsführungsaufgabe. NIS-2 betont ausdrücklich die persönliche Verantwortung der Leitungsorgane für die Einhaltung von Risikomanagement- und Meldepflichten. Der CRA erweitert diese Verantwortung auf die Sicherheit digitaler Produkte über deren gesamten Lebenszyklus.

Damit wird klar: IT-Sicherheit ist kein rein technisches Thema mehr. Sie ist Teil der Unternehmenssteuerung – und integraler Bestandteil eines professionellen Chancen- und Risikomanagements.

Die folgenden Leitprinzipien bieten Orientierung für eine strukturierte Umsetzung im Mittelstand.

SECHS LEITPRINZIPIEN FÜR NIS-2- UND CRA-COMPLIANCE IM MITTELSTAND

1. Strategische Verankerung
Cyberresilienz ist Führungsaufgabe

NIS-2 fordert eine aktive Einbindung der Geschäftsleitung in das Risikomanagement. Delegation ohne Kontrolle genügt nicht.

Unternehmen sollten daher:
- Cyberrisiken explizit in ihre Unternehmensstrategie integrieren
- Zuständigkeiten auf Leitungsebene definieren
- Berichtspflichten und Eskalationsmechanismen etablieren

Die regulatorischen Anforderungen sind dabei nicht isoliert zu betrachten, sondern im Kontext des übergeordneten Chancen- und Risikomanagements. Cyberresilienz ist kein Selbstzweck – sie schützt Wertschöpfung, Reputation und Wettbewerbsfähigkeit.

Stand: Juli 2026

© Der Mittelstand. BVMW e.V. 2026. Alle Rechte vorbehalten. Transparenzregisternummer: 082217218282-59
Der Mittelstand. BVMW e.V. ist unter der Registernummer R001657 eingetragen im Lobbyregister für die Interessensvertretung gegenüber dem Bundestag und der Bundesregierung.

2. Systematisches Risikomanagement
Vom technischen Schutz zur ganzheitlichen Steuerung

NIS-2 verlangt „angemessene und verhältnismäßige technische, operative und organisatorische Maßnahmen".

Dies umfasst insbesondere:
- Risikoanalysen
- Incident-Response-Konzepte
- Business-Continuity-Management
- Lieferketten-Sicherheit
- Dokumentation und Nachweisführung

Hier besteht eine direkte Verbindung zum Impulspapier „Chancen- und Risikomanagement im Mittelstand": Cyberrisiken sind integraler Bestandteil des unternehmerischen Gesamtrisikoprofils und dürfen nicht als isolierte IT-Risiken behandelt werden.

3. Produktsicherheit über den Lebenszyklus (CRA)
Security by Design und Security by Default

Mit dem Cyber Resilience Act werden Hersteller, Importeure und Händler von Produkten mit digitalen Elementen künftig verpflichtet zu:
- Sicherheitsanforderungen bereits in der Entwicklungsphase
- Schwachstellenmanagement
- Sicherheitsupdates über definierte Zeiträume
- Transparenz- und Dokumentationspflichten

Für mittelständische Unternehmen, die Software, IoT-Geräte oder vernetzte Produkte entwickeln oder vertreiben, bedeutet dies einen Paradigmenwechsel: IT-Sicherheit wird zum Produktmerkmal – vergleichbar mit Qualitäts- oder CE-Anforderungen.

4. Organisation, Prozesse und Nachweisfähigkeit
Dokumentation ist Teil der Compliance

Sowohl NIS-2 als auch CRA verlangen belastbare Nachweise.

Empfohlen wird:
- Einführung klarer Governance-Strukturen
- Benennung eines verantwortlichen Informationssicherheitsbeauftragten
- Schulung von Führungskräften
- Aufbau eines internen Kontrollsystems (IKS) für Cyberrisiken

Entscheidend ist nicht nur, dass Maßnahmen existieren – sondern dass sie prüffähig dokumentiert sind.

5. Mensch und Sicherheitskultur
Resilienz entsteht durch Verhalten

Technische Maßnahmen allein genügen nicht. Phishing, Social Engineering und interne Fehlkonfigurationen zählen zu den häufigsten Einfallstoren.

Unternehmen sollten daher:
- regelmäßige Awareness-Schulungen durchführen
- klare Meldewege für Sicherheitsvorfälle definieren
- eine offene Fehler- und Lernkultur fördern

Cyberresilienz ist – wie im Impulspapier zum Chancen- und Risikomanagement beschrieben – ein kontinuierlicher Lernprozess.

6. Umsetzung mit Augenmaß
Proportionalität und Priorisierung

Die Regulierung folgt dem Prinzip der Verhältnismäßigkeit. Nicht jedes Unternehmen benötigt hochkomplexe Sicherheitsarchitekturen.

Empfehlenswert ist ein gestuftes Vorgehen:
- Betroffenheitsanalyse (Fallen wir unter NIS-2?)
- Gap-Analyse zum aktuellen Sicherheitsniveau
- Priorisierung nach Risikoexposition
- Schrittweise Umsetzung mit klaren Meilensteinen

Externe Beratung kann helfen, regulatorische Anforderungen effizient und rechtssicher einzuordnen.

Teil 2: Leitfragen für Unternehmen

Nach der Definition zentraler Prinzipien folgt die Selbstprüfung. Die folgenden Fragen helfen Unternehmen, ihre regulatorische Betroffenheit und ihren Reifegrad realistisch einzuschätzen.

STRATEGISCHE EINORDNUNG

- Fallen wir direkt oder indirekt unter NIS 2?
- Entwickeln oder vertreiben wir Produkte, die unter den CRA fallen?
- Ist Cyberresilienz explizit Teil unserer Unternehmensstrategie?
- Wer trägt auf Geschäftsführungsebene Verantwortung?

© Der Mittelstand. BVMW e.V. 2026. Alle Rechte vorbehalten. Transparenzregisternummer: 082217218282-59
Der Mittelstand. BVMW e.V. ist unter der Registernummer R001657 eingetragen im Lobbyregister für die Interessensvertretung gegenüber dem Bundestag und der Bundesregierung.

RISIKO- UND GOVERNANCE-STRUKTUR

- Haben wir ein dokumentiertes Informationssicherheitsmanagement?
- Wie integrieren wir Cyberrisiken in unser übergeordnetes Risikomanagement?
- Existieren Notfall-, Wiederanlauf- und Meldeprozesse?
- Wie sichern wir unsere Lieferkette ab?

OPERATIVE UMSETZUNG

- Sind unsere technischen Schutzmaßnahmen risikoadäquat?
- Wie schnell erkennen wir Sicherheitsvorfälle?
- Sind Meldefristen organisatorisch abbildbar?
- Wie dokumentieren wir Maßnahmen prüffähig?

PRODUKTSICHERHEIT (RELEVANT FÜR HERSTELLER)

- Berücksichtigen wir Security by Design in Entwicklungsprozessen?
- Gibt es ein strukturiertes Schwachstellenmanagement?
- Sind Update- und Patchprozesse geregelt?
- Können wir Konformität gegenüber Behörden nachweisen?

MENSCH UND KULTUR

- Wie sensibilisiert ist unsere Belegschaft für Cyberrisiken?
- Werden Sicherheitsvorfälle transparent behandelt?
- Fördern wir eine Kultur der kontinuierlichen Verbesserung?

Fazit

NIS 2 und der Cyber Resilience Act sind keine rein regulatorischen Bürden. Richtig umgesetzt, stärken sie die Widerstandsfähigkeit, Reputation und Zukunftsfähigkeit mittelständischer Unternehmen.

Cybersicherheit ist damit nicht nur eine Frage der Compliance, sondern ein strategischer Wettbewerbsfaktor – und integraler Bestandteil eines professionellen Chancen- und Risikomanagements.

Der Mittelstand verfügt über die notwendigen Stärken: kurze Entscheidungswege, unternehmerische Verantwortung und pragmatische Umsetzungskraft.

Dieses Impulspapier soll dazu beitragen, regulatorische Anforderungen nicht als Belastung, sondern als Anlass zur strukturellen Stärkung der eigenen Resilienz zu verstehen – mit Augenmaß, Systematik und strategischer Klarheit.

Rechtlicher Hinweis: Dieses Impulspapier bietet eine allgemeine Orientierung zu NIS 2 und dem Cyber Resilience Act und ersetzt keine auf den Einzelfall bezogene Rechtsberatung. Die dargestellten Inhalte geben den Stand der Diskussion und Regulierung zum Mai 2026 wieder. Für konkrete Maßnahmen und Entscheidungen empfiehlt sich eine Prüfung der jeweiligen Situation unter Hinzuziehung einer zur Rechtsberatung berechtigten Person.

Der Mittelstand. BVMW vertritt mit seinen rund 28.000 Mitglieder in Politik, Medien und Gesellschaft erfolgreich die Interessen des Mittelstands. Mit rund 200 Geschäftsstellen bundesweit und über 85 eigenen Auslandbüros ist der BVMW national sowie international präsent.

Kontakt
Der Mittelstand. BVMW e.V., Politik Inland
Alte Potsdamer Straße 5, 10785 Berlin
Telefon: + 49 30 533206-0, E-Mail: politik@bvmw.de
Social Media: @MittelstandBVMW

© Der Mittelstand. BVMW e.V. 2026. Alle Rechte vorbehalten. Transparenzregisternummer: 082217218282-59
Der Mittelstand. BVMW e.V. ist unter der Registernummer R001657 eingetragen im Lobbyregister für die Interessensvertretung gegenüber dem Bundestag und der Bundesregierung.