Datum

November 2025

Studie im Auftrag des

Bundesministeriums für Wirtschaft und Energie

KI-Verordnung, NIS-2-Richtlinie und Cyber Resilience Act: Auswirkungen auf KMU

Begleitforschung Mittelstand-Digital

RAMBØLL Bright ideas. Sustainable change. IW IW CONSULT

KI-Verordnung, NIS-2-Richtlinie und Cyber Resilience Act: Auswirkungen auf KMU

Begleitforschung Mittelstand-Digital

Ramboll Management Consulting GmbH

Jürgen-Töpfer-Straße 48

22763 Hamburg

www.ramboll.com/de-de

In Zusammenarbeit mit:

Institut der deutschen Wirtschaft Köln e.V.

Konrad-Adenauer-Ufer 21

50668 Köln

Institut der deutschen Wirtschaft Köln Consult GmbH

Konrad-Adenauer-Ufer 21

50668 Köln

Ansprechpersonen

Dr. Thorsten Lübbers; thorsten.luebbers@ramboll.com

Dr. Vera Demary; vera.demary@iwkoeln.de

Autorinnen und Autoren:

Barbara Engels

Dr. Thorsten Lang

Dr. Marc Scheufen

Inhalt

Executive Summary		2
1.	Einleitung	4
2.	Regulatorischer Rahmen	4
2.1	KI-Verordnung – Anwendungsbereich und zentrale Anforderungen	4
2.2	NIS-2-Richtlinie – Anwendungsbereich und zentrale Anforderungen	7
2.3	Cyber Resilience Act – Anwendungsbereich und zentrale Anforderungen	8
2.4	Zusammenspiel von KI-VO, NIS-2, CRA und DSGVO	10
2.4.1	Schnittstellen und Synergien der neuen Regulierungen	11
2.4.2	Potenzielle Zielkonflikte zwischen den Regelwerken	12
3.	Auswirkungen auf KMU – KI-Verordnung	12
3.1	Betroffenheitsanalyse	12
3.2	Ausgangslage der betroffenen Unternehmen	14
3.3	Zentrale Herausforderungen im Kontext der KI-Verordnung	15
3.4	Kosten im Kontext der KI-Verordnung	15
3.5	Nutzen der KI-Verordnung	16
3.6	Unterstützungsbedarfe der KMU	17
3.6.1	Bestehende Unterstützungsangebote	18
3.6.2	Empfehlungen zur Weiterentwicklung	20
4.	Auswirkungen auf KMU – Cybersicherheitsregulierung	20
4.1	Cybersicherheitslage in KMU	20
4.2	NIS-2-Richtlinie	25
4.2.1	Betroffenheitsanalyse	25
4.2.2	Ausgangslage der betroffenen Unternehmen	26
4.2.3	Zentrale Herausforderungen im Kontext der NIS-2-Richtlinie	28
4.2.4	Kosten im Kontext der NIS-2-Richtlinie	29
4.2.5	Nutzen der NIS-2-Richtlinie	30
4.3	Cyber Resilience Act	31
4.3.1	Betroffenheitsanalyse	31
4.3.2	Ausgangslage der betroffenen Unternehmen	33
4.3.3	Zentrale Herausforderungen im Kontext des Cyber Resilience Acts	34
4.3.4	Kosten im Kontext des Cyber Resilience Acts	35
4.3.5	Nutzen des Cyber Resilience Acts	36
4.4	Unterstützungsbedarfe der KMU	36
4.4.1	Bestehende Angebote	37
4.4.2	Empfehlungen für die Weiterentwicklung der Angebote	38
5.	Ausblick	39
Literaturverzeichnis		41

Executive Summary

Die digitale Transformation eröffnet kleinen und mittleren Unternehmen (KMU) neue Chancen, stellt sie jedoch zugleich vor erhebliche regulatorische Herausforderungen. Drei aktuelle EU-Regelwerke – die KI-Verordnung (AI Act), die NIS-2-Richtlinie und der Cyber Resilience Act (CRA) – verändern den Handlungsrahmen für KMU grundlegend.

Alle drei Regelungen sind zentrale Bausteine eines wachsenden europäischen Rechtsrahmens. Sie setzen an unterschiedlichen Punkten an, verfolgen aber das gemeinsame Ziel, ein sicheres, vertrauenswürdiges und wettbewerbsfähiges digitales Binnenmarktgefüge zu schaffen. Die vorliegende Studie stellt die Regelwerke vor, untersucht, inwiefern KMU von ihnen betroffen sind, analysiert Kosten und Nutzen und leitet daraus Unterstützungsbedarfe ab.

Die KI-Verordnung verfolgt das Ziel, den sicheren und grundrechtskonformen Einsatz von KI-Systemen zu gewährleisten und gleichzeitig Innovation zu fördern. Sie klassifiziert KI-Systeme nach Risiko – von „niedrig" bis „inakzeptabel" – und knüpft daran abgestufte Pflichten. Während inakzeptable Systeme verboten sind, unterliegen insbesondere Hochrisiko-Anwendungen strengen Vorgaben wie einem kontinuierlichen Risikomanagement. Die NIS-2-Richtlinie stärkt die Cybersicherheit, indem sie Unternehmen in zahlreichen Sektoren zu umfangreichen organisatorischen und technischen Maßnahmen verpflichtet. Damit sind viele KMU direkt oder über Lieferketten indirekt betroffen. Der CRA schließlich soll die Sicherheit von Produkten mit digitalen Elementen für mindestens fünf Jahre oder für die kürzere Produktlebensdauer gewährleisten. Er verpflichtet Hersteller, Händler und Importeure zu Maßnahmen wie Schwachstellenmanagement, Sicherheitsupdates und umfassender technischer Dokumentation – Anforderungen, die ebenfalls viele KMU betreffen.

Zahlreiche KMU in Deutschland unterliegen diesen neuen Vorgaben. Der Einsatz von KI nimmt rasant zu, insbesondere in Marketing, Vertrieb und IT. Bis zu 160.000 KMU dürften daher zumindest die grundlegenden Pflichten der KI-Verordnung erfüllen müssen. Von NIS-2 sind knapp 30.000 Unternehmen direkt betroffen; über Wertschöpfungsketten könnten für mehr als 200.000 weitere Unternehmen indirekte Verpflichtungen entstehen. Beim CRA ist mit 38.000 bis 120.000 betroffenen Unternehmen zu rechnen. Auffällig ist, dass das Cybersicherheitsniveau zwischen von NIS-2 betroffenen und nicht betroffenen KMU bislang kaum variiert –ein Hinweis darauf, dass viele die NIS-2-Anforderungen noch nicht umgesetzt haben. Zwar ist das deutsche Umsetzungsgesetz noch nicht in Kraft getreten, die Pflichten werden jedoch in naher Zukunft wirksam.

Die neuen Regelungen sind für KMU mit zahlreichen Kosten, aber auch mit Nutzen verbunden. Vorteile ergeben sich durch höheres Vertrauen in digitale Produkte, einen EU-weit einheitlichen Marktzugang und Wettbewerbsvorteile durch zertifizierte Sicherheit. Demgegenüber stehen teils erhebliche Compliance-Kosten, die kurzfristig die Wettbewerbsfähigkeit und Innovationskraft gerade kleinerer Unternehmen belasten können. Langfristig dürften die Vorteile jedoch überwiegen – nicht zuletzt, weil regulierungsbedingte höhere Sicherheitsniveaus die erheblichen wirtschaftlichen Schäden durch Cyberangriffe verringern können.

Die größten Herausforderungen für KMU entstehen durch komplexe Anforderungen, Rechtsunsicherheit, den Fachkräftemangel insbesondere hinsichtlich Cybersicherheitsexpertinnen und -experten sowie Compliance-Fachkräften, eine oft wenig ausgeprägte Sicherheitskultur und begrenzte Ressourcen. Bei der KI-Verordnung besteht insbesondere die Schwierigkeit in der korrekten Risikoklassifizierung von KI-Systemen. Die NIS-2-Richtlinie verlangt umfassende organisatorische Sicherheitsmaßnahmen und strenge Meldepflichten, die in vielen KMU bislang weder technisch noch personell abgebildet sind. Beim CRA liegt die Herausforderung in der dauerhaften Sicherstellung von Update- und Schwachstellenmanagement sowie Dokumentations- und Meldepflichten – ressourcenintensive Prozesse, die insbesondere kleine Unternehmen herausfordern.

Aus diesen Herausforderungen ergeben sich klare Unterstützungsbedarfe: KMU benötigen verlässliche Informationen zu Pflichten und Fristen, praxisnahe Schulungen, branchenspezifische Hilfestellungen sowie eine kontinuierliche Begleitung bei der Umsetzung. Darüber hinaus sind Tools, finanzielle Fördermittel und externe fachliche Unterstützung erforderlich, um Ressourcenengpässe zu überbrücken.

Zwar existiert bereits ein breites Unterstützungsangebot – etwa durch die Mittelstand-Digital Zentren, die Transferstelle Cybersicherheit im Mittelstand oder die European Digital Innovation Hubs (EDIHs). Viele KMU zeigen sich trotzdem überfordert und unsicher und bleiben passiv. Empfehlenswert wäre eine Bündelung bestehender Angebote auf einer zentralen Plattform, ergänzt um eine branchenspezifische Aufbereitung. Zusätzlich sollten die in der KI-Verordnung vorgesehenen Erleichterungen für KMU rasch umgesetzt werden.

Die neuen EU-Regelungen sind anspruchsvoll, eröffnen KMU jedoch auch strategische Chancen. Ihre Umsetzung sollte nicht als reine Pflichtaufgabe verstanden werden, sondern als Investition in Wettbewerbsfähigkeit und Resilienz. Entscheidend ist, dass KMU frühzeitig handeln und dabei von einer koordinierten Unterstützung durch bestehende Mittelstandsprogramme, Politik, Verbände und Kammern profitieren können.

1. Einleitung

Kleine und mittlere Unternehmen (KMU)[1] stehen im Zentrum der digitalen Transformation – und unter wachsendem Anpassungsdruck. Die zunehmende Digitalisierung von Produkten und Dienstleistungen, die stärkere Vernetzung von Liefer- und Wertschöpfungsketten sowie eine wachsende Abhängigkeit von digitalen Infrastrukturen treffen auf ein immer dichteres Netz rechtlicher Vorgaben. Besonders im Bereich der Künstlichen Intelligenz (KI) und der Cybersicherheit hat die Europäische Union (EU) in den vergangenen Jahren wegweisende Regelwerke verabschiedet, die tief in die unternehmerische Praxis eingreifen. Für viele KMU bedeutet das zahlreiche neue Pflichten – aber auch neue Chancen.

Im Zentrum dieser Kurzstudie stehen drei neue EU-Regulierungen: die Verordnung über Künstliche Intelligenz (KI-VO, AI Act), die NIS-2-Richtlinie und der Cyber Resilience Act (CRA). Sie haben unterschiedliche Schwerpunkte: Die KI-Verordnung regelt die sichere und verantwortungsvolle Entwicklung und Nutzung von KI-Systemen, die NIS-2-Richtlinie verpflichtet Unternehmen zu umfassenden organisatorischen Cybersicherheitsmaßnahmen und der CRA legt technische Anforderungen für Produkte mit digitalen Elementen für fünf Jahre, oder – falls kürzer – für die Lebensdauer des Produkts fest. Gemeinsam ist diesen Digitalregulierungen unter anderem, dass sie in hohem Maße KMU adressieren.

Für KMU ergibt sich eine doppelte Herausforderung: Erstens fehlt es ihnen bislang oft an personellen und organisatorischen Ressourcen, etwa an spezialisierten IT-Fachkräften, Rechtskenntnis und etablierten Compliance-Strukturen, um neue regulatorische Vorgaben effizient umzusetzen (Joswig/Kurz, 2025a). Zweitens sind viele KMU eng in digitale Wertschöpfungsnetzwerke eingebunden und damit häufig indirekt betroffen, selbst wenn sie formal nicht unmittelbar unter eine Regulierung fallen sollten.

Ziel dieser Studie ist es, die Auswirkungen der drei Regelwerke auf KMU in Deutschland systematisch zu erfassen – insbesondere in Bezug auf Betroffenheit, Herausforderungen, Kosten und Nutzen – und darauf aufbauend den konkreten Unterstützungsbedarf für KMU abzuleiten. Die Ergebnisse sollen dazu beitragen, Unterstützungsangebote gezielt (weiter) zu entwickeln und KMU wirksam bei der Umsetzung der neuen Anforderungen zu begleiten.

2. Regulatorischer Rahmen

In diesem Kapitel werden zunächst die Anwendungsbereiche und Anforderungen der EU-Regelwerke KI-Verordnung, NIS-2-Richtlinie und Cyber Resilience Act vorgestellt. Anschließend werden Schnittstellen zu bestehenden Vorgaben wie der DSGVO sowie mögliche Synergien und Konflikte unter den EU-Regelwerken aufgezeigt.

2.1 KI-Verordnung – Anwendungsbereich und zentrale Anforderungen

Die europäische KI-Verordnung (Verordnung (EU) 2024/1689; Verordnungstext: EU, 2024a) verfolgt als weltweit erste umfassende Regulierung für KI das Ziel, Vertrauen in KI zu stärken, Risiken zu minimieren und zugleich Innovationen zu fördern. Im Mittelpunkt steht der menschenzentrierte, transparente und sichere Einsatz von KI-Systemen unter Wahrung von Gesundheit, Sicherheit und Grundrechten der Nutzerinnen und Nutzer.

Die Verordnung trat am 1. August 2024 in Kraft. Erste Pflichten, darunter das Verbot inakzeptabler KI-Systeme (z.B. für biometrische Echtzeitüberwachung) sowie Schulungsvorgaben, gelten seit

[1] In dieser Studie gelten Unternehmen mit bis zu 249 Beschäftigten als KMU. An einzelnen Stellen – etwa bei der Darstellung von Statistik- oder Befragungsergebnissen – werden jedoch abweichende Abgrenzungen verwendet, da in den verwendeten Quellen andere Abgrenzungen zugrunde gelegt wurden; diese werden jeweils kenntlich gemacht.

dem 2. Februar 2025. Im Besonderen sind auch KMU verpflichtet, sicherzustellen, dass Mitarbeitende, die mit KI-Systemen arbeiten, über ein ausreichendes Maß an KI-Kompetenzen verfügen. Diese umfassen technisches Grundverständnis, die Kenntnis rechtlicher und ethischer Rahmenbedingungen sowie die Fähigkeit, Risiken zu erkennen und verantwortungsvoll mit ihnen umzugehen. Der Aufbau dieser Kompetenzen darf flexibel und kontextbezogen gestaltet werden, was insbesondere vor dem Hintergrund begrenzter Ressourcen von KMU betont wird. Die Schulungsmaßnahmen (z.B. interne Schulungen, Richtlinien oder externe Weiterbildungsangebote) müssen dokumentiert und regelmäßig überprüft werden. Die Einhaltung wird ab August 2026 durch nationale Aufsichtsbehörden kontrolliert. Weitere Regelungen, etwa zu General-Purpose-KI und zu Aufsichtsstrukturen, folgten am 2. August 2025. Bis zu diesem Zeitpunkt mussten die Mitgliedstaaten Aufsichtsstrukturen eingerichtet und die zuständigen Behörden für Marktüberwachung, Durchsetzung und Sanktionen benannt haben. In Deutschland läuft dieser Umsetzungsprozess noch.

Die KI-Verordnung richtet sich an sämtliche Akteure, die KI-Systeme in der EU entwickeln oder entwickeln lassen, in Verkehr bringen, betreiben oder nutzen – darunter Anbieter, Nutzerinnen und Nutzer (Betreiber), Importeure und Händler.[2] Anbieter sind natürliche oder juristische Personen oder öffentliche Stellen, die ein KI-System entwickeln oder entwickeln lassen und es unter eigenem Namen oder eigener Marke in Verkehr bringen oder in Betrieb nehmen. Nutzerinnen und Nutzer (Betreiber) sind diejenigen, die ein KI-System unter ihrer Verantwortung einsetzen. Die private, nicht-berufliche Nutzung fällt nicht unter die Betreiberpflichten. Ein KI-System im Sinne der Verordnung ist ein maschinenbasiertes System, das mit unterschiedlichen Autonomiegraden arbeiten kann und nach der Inbetriebnahme anpassungsfähig sein kann. Es leitet für explizite oder implizite Ziele aus Eingaben Ausgaben ab – etwa Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen –, die physische oder virtuelle Umgebungen beeinflussen können. Die KI-Verordnung gilt sektorübergreifend für private und öffentliche Stellen. KMU fallen damit auch dann unter die Verordnung, wenn sie KI in ihrem Unternehmen einsetzen – insbesondere, wenn es sich um regulierte (z. B. hochriskante) KI-Systeme handelt. Die KI-Verordnung hat einen risikobasierten Ansatz: Je höher das Risiko für Nutzerinnen und Nutzer oder die Allgemeinheit, desto stärker die Regulierung des jeweiligen KI-Systems. Dabei unterscheidet die Verordnung vier Risikoklassen[3]:

- KI-Systeme mit niedrigem Risiko – das sind die meisten KI-Systeme – unterliegen keinen verpflichtenden Vorgaben. Die Verordnung sieht hier lediglich die Möglichkeit eines freiwilligen Verhaltenskodex vor. Beispiele sind etwa unternehmensinterne KI-Anwendungen zur Effizienzsteigerung oder Assistenzsysteme für administrative Tätigkeiten wie automatische E-Mail-Zusammenfassungen und Textassistenzanwendungen.
- KI-Systeme mit begrenztem Risiko unterliegen bestimmten Transparenzpflichten. Nutzerinnen und Nutzer müssen darüber informiert werden, dass sie mit einer KI interagieren oder KI-generierte Inhalte (Audio-, Bild-, Video- oder Textinhalte) konsumieren. Beispiele sind Chatbots und Empfehlungssysteme. Zusätzliche Informationspflichten gelten bei Emotionserkennung sowie bei der Erstellung manipulativer Inhalte wie Deepfakes.
- KI-Systeme mit hohem Risiko (im Folgenden Hochrisiko-KI) unterliegen strengen Anforderungen wie einem umfassenden Risikomanagement, technischer Dokumentation, menschlicher Aufsicht, Schulungen und Transparenzpflichten. Schwerwiegende Vorfälle sind meldepflichtig. Beispiele sind KI-Systeme in kritischer Infrastruktur (z. B. Energieversorgung oder Verkehr), KI-gestützte Medizinprodukte zur Diagnose (z. B. Radiologie) oder zur Behandlung von Patienten sowie KI-Anwendungen im Personalmanagement, insbesondere bei der Bewerberauswahl.

[2] Zur besseren Lesbarkeit werden natürliche Personen in weiblicher und männlicher Form bezeichnet, Organisationen in männlicher.

[3] Eine Ausnahme bilden sogenannte „General Purpose AI" (GPAI)-Modelle, wie etwa große Sprachmodelle. Anders als klassische KI-Systeme werden sie nicht nach einem konkreten Einsatz klassifiziert, sondern unterliegen speziellen Vorgaben, die sich am potenziellen systemischen Risiko orientieren. Bei besonders leistungsstarken GPAI-Modellen („high-impact GPAI") richtet sich die Einstufung unter anderem nach der für das Training eingesetzten Rechenleistung sowie dem breiten Anwendungspotenzial.

- KI-Systeme mit inakzeptablem Risiko sind in der EU verboten. Beispiele sind Social-Scoring-Systeme (Bewertung des Verhaltens von Personen) durch Behörden oder Unternehmen, Echtzeit-biometrische Fernidentifikation im öffentlichen Raum oder Emotionserkennung in Schulen und am Arbeitsplatz.

Insbesondere Hochrisiko-KI-Systeme – die auch bei KMU[4] zum Einsatz kommen (Engels et al., 2025) – unterliegen umfangreichen Pflichten. Dazu zählen:

- Risikomanagementsystem: Kontinuierliche Identifikation, Bewertung und Minderung von Risiken.
- Daten und Daten-Governance: Verwendung hochwertiger, repräsentativer und fehlerfreier Trainingsdaten.
- Technische Dokumentation: Nachweis der Konformität des Systems.
- Aufzeichnungspflichten: Protokollierung relevanter Ereignisse während des gesamten Lebenszyklus.
- Transparenz- und Bereitstellungspflichten: Information der Nutzerinnen und Nutzer über Funktionsweise und Grenzen des Systems.
- Menschliche Aufsicht: Mechanismen zur wirksamen menschlichen Kontrolle.
- Genauigkeit, Robustheit und Cybersicherheit: Schutz vor Manipulation und Angriffen.

Diese Anforderungen sind durch ein Konformitätsbewertungsverfahren zu verifizieren, das je nach System intern oder durch eine benannte externe Stelle erfolgt.

Die Nichteinhaltung der Vorschriften – insbesondere bei Hochrisiko- oder verbotenen KI-Systemen – kann erhebliche rechtliche und finanzielle Folgen haben. Die Verordnung sieht drei abgestufte Sanktionshöhen vor, abhängig von Art des Verstoßes und Unternehmensumsatz. Bei Verstößen gegen Pflichten für Hochrisiko-KI drohen Bußgelder von bis zu 15 Millionen Euro oder 3 Prozent des weltweiten Jahresumsatzes. Diese Sanktionsmechanismen sind mit denen der DSGVO vergleichbar und verdeutlichen die Relevanz wirksamer Compliance-Maßnahmen im KI-Bereich.

Für KMU bieten bestehende Normen eine wichtige Orientierung, um die Anforderungen der KI-Verordnung systematisch und ressourcenschonend umzusetzen. Die ISO 42001 definiert erstmals ein international anerkanntes Managementsystem für Künstliche Intelligenz (Artificial Intelligence Management System, AIMS) und unterstützt Unternehmen bei der strukturierten Governance und Dokumentation ihrer KI-Anwendungen. Ergänzend liefert die ISO 23894 einen Standard für das Risikomanagement über den gesamten Lebenszyklus von KI-Systemen – insbesondere relevant für Hochrisiko-KI.

Zusätzlich zu diesen international etablierten Standards bietet die deutsche DIN SPEC 92001-Reihe praxisorientierte Leitlinien zur Qualitätssicherung von KI-Systemen. Teil 1 beschreibt ein Qualitäts-Metamodell mit Fokus auf Funktionalität, Robustheit und Nachvollziehbarkeit. Teil 2 konkretisiert Anforderungen an die Robustheit von KI gegenüber fehlerhaften oder manipulierten Eingaben. Teil 3 liefert Ansätze zur Erklärbarkeit von KI-Entscheidungen und adressiert damit ein zentrales Anliegen der KI-Verordnung.

Insgesamt schaffen die genannten Normen eine Grundlage für KMU, um ihre KI-Systeme rechtskonform zu gestalten. Die DIN SPEC 92001-Reihe kann dort ergänzen, wo Unternehmen gezielt an einzelnen Qualitätsmerkmalen arbeiten möchten – auch ohne formalisierte Zertifizierungsprozesse.

[4] Siehe weiterführend Abschnitt 3.1.

2.2 NIS-2-Richtlinie – Anwendungsbereich und zentrale Anforderungen

Die Richtlinie (EU) 2022/2555 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der EU – kurz NIS-2-Richtlinie – bildet einen zentralen Baustein der europäischen Cybersicherheitsarchitektur (Richtlinientext: EU, 2022a). Sie löst die bisherige NIS-1-Richtlinie (EU) 2016/1148 ab und verfolgt das Ziel, in der gesamten EU ein konsistentes, hohes Schutzniveau für Netz- und Informationssysteme sicherzustellen (Europäische Kommission, 2025a). Die Mitgliedstaaten waren verpflichtet, die NIS-2-Richtlinie bis zum 17. Oktober 2024 in nationales Recht umzusetzen. In Deutschland erfolgt dies durch das geplante „Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung", kurz NIS-2-Umsetzungsgesetz. Es wird das Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) neu strukturieren und stark erweitern. Außerdem werden noch mehr als 20 weitere Gesetze und Verordnungen überarbeitet, die teils branchenspezifische Sonderregelungen enthalten, darunter das Telekommunikationsgesetz. Ein entsprechender Gesetzentwurf wurde am 30. Juli 2025 vom Kabinett verabschiedet, das Gesetzgebungsverfahren ist jedoch noch nicht abgeschlossen und befindet sich nach erstmaliger Beratung im Bundestag am 11. September 2025 noch im parlamentarischen Verfahren (BMI, 2025).

Gegenüber der Vorgängerrichtlinie wurde der Adressatenkreis deutlich erweitert. Statt der früheren engen Kategorien „Betreiber kritischer Infrastrukturen" (jetzt „Betreiber kritischer Anlagen") und „digitale Diensteanbieter" unterscheidet NIS-2 nun in der Wirtschaft zwischen besonders wichtigen Einrichtungen und wichtigen Einrichtungen. Besonders wichtige Einrichtungen sind vor allem große Unternehmen in den Sektoren Energie, Transport und Verkehr, Finanzwesen, Gesundheit, Wasser, digitale Infrastruktur und Weltraum. Wichtige Einrichtungen sind mittlere Unternehmen dieser Sektoren sowie mittlere und große Unternehmen in den Sektoren Abfallbewirtschaftung, Chemie, Ernährung, Verarbeitendes Gewerbe, Anbieter digitaler Dienste und Forschung. In den Anhängen der NIS-2-Richtlinie werden die Sektoren noch detaillierter nach einzelnen Branchen und Arten von Einrichtungen differenziert. Als groß gilt ein Unternehmen, wenn es mindestens 250 Beschäftigte hat oder sowohl einen Jahresumsatz von mehr als 50 Millionen Euro als auch eine Jahresbilanzsumme von über 43 Millionen Euro erreicht. Ein mittleres Unternehmen hat mindestens 50 Beschäftigte oder einen Jahresumsatz und eine Jahresbilanzsumme von jeweils über 10 Millionen Euro. Darüber hinaus gibt es allerdings zahlreiche Sonderfälle und Ausnahmen.

Unternehmen, die unter die NIS-2-Richtlinie fallen, sind verpflichtet, ein hohes Maß an betrieblicher Cybersicherheit sicherzustellen. Im Zentrum steht die Einführung eines systematischen Risikomanagements, in der Regel über ein Informationssicherheits-Managementsystem (ISMS), sowie die Umsetzung angemessener, dem Stand der Technik entsprechender technischer und organisatorischer Schutzmaßnahmen. Dazu gehören mehrstufige Zugangskontrollen, sichere Authentifizierungsverfahren, ein kontinuierliches Schwachstellenmanagement und ein strukturiertes Patch-Management, also die zeitnahe Installation von Sicherheitsupdates zur Schließung bekannt gewordener Sicherheitslücken. Mitarbeitende müssen regelmäßig geschult und für Cybersicherheitsrisiken sensibilisiert werden. Auch Risiken entlang der Lieferkette müssen bewertet und durch geeignete vertragliche und technische Maßnahmen bei Dienstleistern und Zulieferern abgesichert werden. Zusätzliche Sicherheitsanforderungen gelten für Betreiber kritischer Anlagen, die zum Einsatz von Systemen zur Angriffserkennung verpflichtet sind.

Darüber hinaus verpflichtet die NIS-2-Richtlinie Unternehmen, erhebliche IT-Sicherheitsvorfälle innerhalb definierter Fristen an die zuständigen Behörden zu melden. Dafür sind interne Meldeprozesse und klare Zuständigkeiten, insbesondere auf Managementebene, zu etablieren. Die Unternehmensleitung trägt eine besondere Verantwortung: Sie ist für die Einhaltung der Vorschriften rechenschaftspflichtig, muss regelmäßig geschult werden und kann bei grober Pflichtverletzung persönlich haftbar gemacht werden.

Ergänzt werden diese Anforderungen durch eine umfassende Dokumentations- und Nachweispflicht. Sämtliche umgesetzten Sicherheitsmaßnahmen, Zuständigkeiten und Risikoanalysen müssen nachvollziehbar dokumentiert und den Aufsichtsbehörden auf Verlangen vorgelegt werden.

Insgesamt unterscheiden sich die Anforderungen nach Einstufung: Besonders wichtige Einrichtungen unterliegen strengeren Pflichten, insbesondere bei Aufsicht und Sanktionen. Bei ihnen sind sowohl proaktive Prüfungen durch Aufsichtsbehörden möglich (ex-ante) als auch höhere Bußgeldrahmen vorgesehen (bis zu 10 Millionen Euro oder 2 Prozent des weltweiten Jahresumsatzes). Wichtige Einrichtungen werden in der Regel anlassbezogen geprüft (ex-post) und unterliegen geringeren Höchststrafen (bis zu 7 Millionen Euro oder 1,4 Prozent des weltweiten Jahresumsatzes).

Unternehmen, die als Kritische Infrastruktur (KRITIS) eingestuft sind, unterliegen zusätzlich dem künftigen KRITIS-Dachgesetz, das zur Umsetzung der europäischen CER-Richtlinie (Critical Entities Resilience) in nationales Recht überführt wird. Dieses Gesetz ergänzt die NIS-2-Richtlinie um Anforderungen zur physischen Resilienz, insbesondere in den Bereichen Zugangsschutz, Notfallvorsorge und der Absicherung von Standorten. Unternehmen, die unter beide Regelwerke fallen, müssen IT- und physische Sicherheitsmaßnahmen koordiniert und integriert umsetzen. Im Falle sich überschneidender oder widersprechender Anforderungen vom KRITIS-Dachgesetz und von NIS-2-Umsetzungsgesetz drohen unnötige Bürokratie, Effizienzverluste und Rechtsunsicherheiten; daher ist eine aufeinander abgestimmte Umsetzung der beiden europäischen Richtlinien in deutsches Recht wichtig. Diese Kritik wurde bereits im Deutschen Bundestag (2024) geäußert. Seitdem hat sich die Lage jedoch weiterentwickelt: Am 10. September 2025 hat das Bundeskabinett den Gesetzentwurf zum KRITIS-Dachgesetz verabschiedet.

Angesichts der hohen regulatorischen Anforderungen bieten etablierte Sicherheitsstandards eine wertvolle Orientierungshilfe. Eine Zertifizierung nach ISO 27001 gilt als anerkannte Grundlage zur Umsetzung der NIS-2-Vorgaben, da sie ein strukturiertes Informationssicherheits-Managementsystem umfasst, das Risiken systematisch identifiziert, geeignete Schutzmaßnahmen gemäß ISO 27002 implementiert und kontinuierliche Verbesserungsprozesse vorsieht. Allerdings deckt ISO 27001 nicht alle Anforderungen der NIS-2-Richtlinie ab. Ergänzende Pflichten wie Meldeverfahren, Kontaktstellen zu Behörden, Rechenschaftspflicht auf Geschäftsleitungsebene und Management-Schulungen müssen zusätzlich berücksichtigt werden (OpenKRITIS, 2024a). Eine Übersicht über die Zuordnung einzelner NIS-2-Anforderungen zu bestehenden Sicherheitsstandards bietet OpenKRITIS (2024b).

Eine TISAX-Zertifizierung, wie sie insbesondere in der Automobilindustrie verbreitet ist, bestätigt ebenfalls die Wirksamkeit eines ISMS sowie die Einhaltung definierter Schutzniveaus. Laut einer Analyse der ENX Association (2025), die das TISAX-System verwaltet, erfüllen TISAX-zertifizierte Unternehmen bereits nahezu alle wesentlichen NIS-2-Anforderungen, mit Ausnahme der formellen Meldepflichten und der aufsichtsrechtlichen Nachweispflichten.

Für kleinere Unternehmen, die (noch) nicht unter die Pflichten der NIS-2-Richtlinie fallen, bietet die im Förderprojekt „mIT Standard sicher" des Bundesministeriums für Wirtschaft und Energie (BMWE) entwickelte DIN SPEC 27076 eine praxisnahe Einstiegshilfe in die betriebliche IT-Sicherheit (DIN, 2023). Sie ermöglicht auf Grundlage eines standardisierten Cyber-Risiko-Checks eine erste strukturierte Absicherung und kann gezielt auf weiterführende Zertifizierungen wie ISO 27001 oder TISAX oder auf eine spätere Einstufung als wichtige Einrichtung vorbereiten.

2.3 Cyber Resilience Act – Anwendungsbereich und zentrale Anforderungen

Mit der Verordnung (EU) 2024/2847 über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen – dem Cyber Resilience Act (CRA) – verfolgt die EU das Ziel, einheitliche und verbindliche Sicherheitsstandards für digitale Produkte zu schaffen (Verordnungstext: EU, 2024b). „Horizontal" bedeutet dabei, dass die Anforderungen branchen- und produktübergreifend gelten – unabhängig vom Anwendungsbereich. Die Verordnung trat am 10. Dezember 2024 in Kraft und ist ab dem 11. Dezember 2027 unmittelbar in allen Mitgliedstaaten anzuwenden.

Der CRA soll die Cybersicherheit von Produkten mit digitalen Elementen für fünf Jahre, oder – falls kürzer – für die Lebensdauer des Produkts, gewährleisten und gleichzeitig den Binnenmarkt durch die Schaffung eines einheitlichen Rechtsrahmens stärken. Er reagiert auf das oft unzureichende Sicherheitsniveau digitaler Produkte – etwa durch fehlende Schwachstellenbehebungen – und adressiert die mangelnde Transparenz für Endnutzerinnen und -nutzer hinsichtlich Sicherheitsmerkmalen und -risiken.

Unter den Begriff „Produkte mit digitalen Elementen" fallen laut CRA alle Produkte, die mit einem Gerät oder Netzwerk verbunden werden können, also sowohl vernetzbare Hardware (darunter beispielsweise Smartphones, Smart-Home-Geräte, Mikroprozessoren, Firewalls und intelligente Zähler) als auch Softwareprodukte (darunter beispielsweise Buchhaltungsprogramme, Computerspiele oder mobile Apps) (BSI, 2025b). Ausgenommen sind sektorspezifisch regulierte Produktkategorien wie medizinische Geräte, Fahrzeuge sowie Luft- und Seefahrttechnik. Eine Lex-Specialis-Klausel[5] stellt sicher, dass in solchen Fällen keine Doppelregulierung entsteht.

Die Adressaten des CRA sind alle Wirtschaftsakteure unabhängig von der Unternehmensgröße, die Produkte mit digitalen Elementen auf dem EU-Binnenmarkt herstellen, einführen, vertreiben oder bereitstellen. Die konkreten Pflichten, die der CRA vorsieht, hängen davon ab, welche der Rollen (Hersteller, Einführer, Händler) eine Organisation in Bezug auf ein Produkt einnimmt:

- Hersteller tragen die Verantwortung für die Einhaltung der CRA-Anforderungen. Sie müssen Produkte nach den Prinzipien Security by Design und Security by Default entwickeln, eine Risikobewertung durchführen, eine technische Dokumentation erstellen, regelmäßige Sicherheitsupdates für mindestens fünf Jahre, oder falls kürzer, über den gesamten Produktlebenszyklus hinweg, sicherstellen und ein System zum Schwachstellenmanagement etablieren. Schwerwiegende Schwachstellen müssen binnen 24 Stunden an die EU-Cybersicherheitsagentur ENISA gemeldet werden. Die CE-Kennzeichnung dokumentiert die Konformität des Produkts mit dem CRA.
- Einführer müssen vor dem Inverkehrbringen auf dem Binnenmarkt sicherstellen, dass das Produkt alle CRA-Vorgaben erfüllt. Sie sind zur Prüfung der Konformität verpflichtet und müssen die technische Dokumentation vorhalten.
- Händler dürfen nur Produkte vertreiben, die den Vorschriften des CRA entsprechen – insbesondere hinsichtlich CE-Kennzeichnung und mitgelieferter Sicherheitsinformationen. Wenn Händler Produkte unter eigenem Namen vertreiben oder wesentlich verändern, gelten sie rechtlich als Hersteller und unterliegen denselben Pflichten.

Bei Verstößen gegen den CRA drohen empfindliche Sanktionen, die bis zu 15 Millionen Euro oder 2,5 Prozent des weltweiten Jahresumsatzes eines Unternehmens betragen können.

Bestehende Normen erleichtern – wie auch bei NIS-2 und bei der KI-Verordnung – bereits jetzt teilweise die Einhaltung der weitreichenden Pflichten. Viele CRA-Anforderungen werden durch bestehende Normen zumindest teilweise adressiert (JRC/ENISA, 2024). Dazu zählen Risikobewertung (ISO 27005), Authentifizierung und Zugangskontrollen (ISO 27002), Security-by-Design (IEC 62443 für industrielle Steuerungssysteme) sowie Minimierung der Angriffsfläche und sichere Datenverarbeitung (EN 303 645 für Internet of Things (IoT)-Verbraucherprodukte). Allerdings deckt keine einzelne Norm den CRA vollständig ab, und viele der Normen sind nicht auf alle vom CRA erfassten Produkte übertragbar. Insbesondere bestehen Lücken bei automatisierten Sicherheitsupdates, den Meldepflichten und produktbezogenen Nachweisanforderungen. Zur Schließung dieser Lücken wurde ein Standardisierungsprozess gestartet (vgl. stan4cra.eu (CEN/CENELEC/ETSI, 2025)). Erste harmonisierte Standards werden 2026 erwartet. Zusätzlich bietet das freiwillige IT-Sicherheitskennzeichen des BSI, das schrittweise an die CRA-Ziele angepasst wird, eine frühe Orientierung für Hersteller bereits im Entwicklungsprozess (BSI, 2025b), wenngleich dieses nicht von der Verpflichtung der Erfüllung der CRA-Anforderungen entbindet.

[5] Die Lex-Specialis-Klausel besagt, dass im Konfliktfall zwischen zwei Rechtsnormen die speziellere Norm Vorrang vor der allgemeineren hat.

2.4 Zusammenspiel von KI-VO, NIS-2, CRA und DSGVO

Die drei EU-Regelwerke – KI-Verordnung, NIS-2-Richtlinie und Cyber Resilience Act – sind zentrale Bausteine eines wachsenden regulatorischen Rahmens im Kontext der europäischen Datenökonomie, Digitalstrategie und Cybersicherheitsarchitektur. Ausgangspunkt dieser Entwicklung war die Datenschutz-Grundverordnung (DSGVO), die im Mai 2018 in Kraft getreten ist. Auf die DSGVO wird im Folgenden als Vergleich immer wieder Bezug genommen, da sie als erstes umfassendes EU-Regelwerk alle Unternehmen – einschließlich KMU – betroffen hat und Maßstäbe für Umsetzung und Compliance gesetzt hat.

Alle Regulierungen setzen an unterschiedlichen Stellen an, verfolgen aber das gemeinsame Ziel, ein sicheres, vertrauenswürdiges und wettbewerbsfähiges digitales Binnenmarktgefüge zu schaffen. Oft steht eine Meldepflicht im Zentrum, deren Auslöser, Fristen und Adressaten variieren. Unternehmen, insbesondere KMU, sind daher oft gleichzeitig mehreren Regelungen unterworfen (Tabelle 2-1).

Tabelle 2-1: Übersicht zentraler EU-Digitalregulierungen

	KI-VO	NIS-2	CRA	DSGVO
Ziel	Grundrechtskonformer, transparenter und sicherer Einsatz von KI	Sicherstellung der Cybersicherheit von Unternehmen	Sicherstellung der Cybersicherheit von Produkten mit digitalen Elementen, Transparenz	Schutz personenbezogener Daten, informationelle Selbstbestimmung
Primärer Anknüpfungspunkt	Herstellung, Entwicklung, Bereitstellung und Nutzung bestimmter KI-Systeme	Von Unternehmen erbrachte Tätigkeiten und Dienste	Mindestens fünf Jahre oder, falls kürzer, gesamter Produktlebenszyklus (Hardware/Software)	Verarbeitung personenbezogener Daten
Typischer Adressat	Alle Unternehmen, die in der EU genannte Technologien anbieten/nutzen	Unternehmen bestimmter Größe in bestimmten Sektoren	Hersteller, Einführer, Händler	Verantwortliche und Auftragsdatenverarbeiter, die personenbezogene Daten von EU-Bürgern verarbeiten
Meldepflicht	Schwerwiegende Vorkommnisse	Erheblicher Schaden	Kenntnis einer aktiv ausgenutzten signifikanten Schwachstelle	Datenschutzverletzung
Frist	15 Tage nach Feststellung; bei schweren und unumkehrbaren Störungen kritischer Infrastrukturen 48 Stunden; bei Todesfall 10 Tage	24 Stunden Frühwarnung; 72 Stunden Detailmeldung; Abschlussbericht nach einem Monat	24 Stunden Frühwarnung; 72 Stunden Detailmeldung; nach 14 Tagen Bericht über Korrektur- oder Risikominderungsmaßnahme	Unverzüglich, spätestens jedoch 72 Stunden nach Bekanntwerden
Meldebehörde	Bundesnetzagentur als Marktüberwachungsbehörde vorgesehen	Bundesamt für Sicherheit in der Informationstechnik (BSI)	BSI	Landesdatenschutzbehörden

Ausgewählte Regulierungen, Stand: Oktober 2025

Quelle: Eigene Darstellung

Oft überschneiden sich die Anwendungsbereiche der Regelwerke. Ein fiktives Beispiel ist ein Unternehmen mit weniger als 50 Beschäftigten, das ein KI-gestütztes Diagnosesystem entwickelt und an Krankenhäuser als Software-as-a-Service (SaaS) vertreibt:

- KI-VO: Hochrisiko-KI-System aufgrund des Einsatzes im Gesundheitsbereich.
- CRA: Produkt mit digitalen Elementen unterliegt produktsicherheitsrechtlichen Cybersicherheitsanforderungen.

- NIS-2: Indirekte Betroffenheit über angebundene Krankenhäuser als „besonders wichtige Einrichtungen".
- DSGVO: Verarbeitung sensibler Patientendaten, falls Daten auf Servern des Betreibers gespeichert werden.

Im Falle eines Cyberangriffs auf Patientendaten könnten mehrere Meldepflichten greifen – jedoch mit unterschiedlichen Auslösern:

- DSGVO: Jede Datenschutzverletzung ist meldepflichtig.
- NIS-2: Meldung nur bei erheblichem Schaden.
- CRA: Meldung bei Kenntnis einer aktiv ausgenutzten signifikanten Schwachstelle.

Diese Pflichten können parallel entstehen, betreffen aber nicht zwangsläufig dieselben Akteure: Während die DSGVO und NIS-2 typischerweise den Betreiber eines Systems adressieren, richtet sich der CRA primär an den Hersteller – es sei denn, das Unternehmen vertreibt und betreibt das Produkt selbst, etwa im Rahmen eines SaaS-Modells. In solchen Fällen greifen alle Meldepflichten gleichzeitig, was insbesondere für KMU einen hohen Abstimmungsaufwand bedeutet. Ein zentralisiertes Meldeverfahren könnte hier Entlastung schaffen (Hessel, 2025).

2.4.1 Schnittstellen und Synergien der neuen Regulierungen

Die KI-Verordnung, der CRA und die NIS-2-Richtlinie führen in der Praxis – zusätzlich zu den oben aufgezeigten Meldepflichten bei Datenschutzverletzungen gemäß DSGVO – zu kumulativen Pflichten. Besonders deutlich wird dies im Zusammenspiel von KI-VO und CRA: Enthält ein Produkt mit digitalen Elementen – etwa ein IoT-Gerät mit Bilderkennung oder eine Software mit automatisierter Entscheidungslogik – KI-Funktionalitäten, greifen beide Regelwerke gleichzeitig. Während der CRA die Cybersicherheit des Produkts über fünf Jahre beziehungsweise, falls kürzer, die Produktlebensdauer, regelt, stellt die KI-VO Anforderungen an Transparenz, Nachvollziehbarkeit und die Risikoklassifikation des eingesetzten KI-Systems.

Auch zwischen KI-VO und NIS-2 können sich Pflichten überlagern. Dies ist etwa der Fall, wenn KI-Systeme zur Absicherung digitaler Infrastrukturen genutzt werden und gleichzeitig selbst als Hochrisiko-KI gelten. In einem solchen Szenario müssen Anbieter sowie Nutzerinnen und Nutzer nicht nur die Sicherheits- und Dokumentationsvorgaben der NIS-2-Richtlinie erfüllen, sondern auch die Transparenz-, Aufsichts- und Qualitätsanforderungen der KI-VO einhalten.

Zwischen den beiden Cybersicherheitsregulierungen gibt es ebenfalls Berührungspunkte. Die NIS-2-Richtlinie verpflichtet betroffene Unternehmen zur Absicherung ihrer betrieblichen IT, der CRA hingegen regelt die Sicherheit digitaler Produkte. Mittlere Unternehmen ab 50 Beschäftigten (oder mit einem Umsatz von mindestens 10 Millionen Euro) sind häufig von beiden Regimen erfasst – etwa, wenn sie als Teil eines NIS-2-Sektors die NIS-2-Schwellenwerte (Beschäftigtenzahl, Umsatz oder Bilanzsumme) überschreiten und zugleich digitale Produkte herstellen, vertreiben oder importieren. So greifen bei einem Produkt mehrere Anforderungen: Unternehmen müssen ihre internen Systeme als Betreiber regelmäßig aktualisieren und absichern (NIS-2), und gleichzeitig als Hersteller sicherstellen, dass CRA-relevante Produkte mit Sicherheitsupdates versorgt werden. Zudem gibt es mehrere Meldepflichten: Sicherheitsvorfälle sind sowohl im Betrieb als auch im Produktkontext zu adressieren. Verantwortung und Rechenschaftspflichten des Managements bestehen in beiden Regelwerken.

Gleichzeitig eröffnen sich durch die Parallelität der Vorgaben Synergien. Ein gutes internes Sicherheitsniveau (NIS-2) ist Voraussetzung, um sichere Produkte zu entwickeln (CRA) – und sichere Produkte reduzieren wiederum die Risiken im eigenen Betrieb und bei Kunden. CRA-konforme Hard- und Software erleichtert die Umsetzung der NIS-2-Pflichten. Zwar unterscheiden sich die Meldepflichten und die erforderlichen Kenntnisse (NIS-2 adressiert vor allem betriebliche Prozesse und Managementsysteme, der CRA hingegen produktspezifische Sicherheitsaspekte), doch können etablierte Strukturen wie Incident-Response-Teams oder interne Meldeprozesse wechselseitig genutzt werden.

Um diese Synergiepotenziale zu heben und ineffiziente Doppelstrukturen zu vermeiden, ist eine koordinierte Umsetzung beider Regelwerke durch die betroffenen Unternehmen notwendig. Integrierte Compliance-Programme – etwa ein Informationssicherheits-Managementsystem, das beide Regelwerke berücksichtigt – ermöglichen eine effizientere Umsetzung. Wie in den Abschnitten 2.2 und 2.3 dargestellt, decken viele etablierte Normen zentrale Anforderungen sowohl von NIS-2 als auch vom CRA ab. Eine harmonisierte Anwendung dieser Standards kann gerade KMU wirksam entlasten.

2.4.2 Potenzielle Zielkonflikte zwischen den Regelwerken

Die parallele Anwendung mehrerer Rechtsakte kann nicht nur zu organisatorischem Mehraufwand, sondern auch zu inhaltlichen Spannungen führen. So verlangt die KI-VO für Hochrisiko-KI hochwertige, repräsentative und vollständige Datensätze für Training, Validierung und Testung, während die DSGVO das Prinzip der Datenminimierung vorgibt – eine Anforderung, die insbesondere bei sensiblen Daten zu schwierigen Abwägungen führen kann (Winau, 2023). Teilweise kann der Konflikt durch Anonymisierung oder synthetische Daten entschärft werden.

Auch im Bereich der Entscheidungsprozesse gibt es Überschneidungen: Die KI-VO schreibt menschliche Aufsicht bei Hochrisiko-KI-Systemen vor, wohingegen Artikel 22 DSGVO nur dann greift, wenn eine Entscheidung ausschließlich automatisiert erfolgt. Daraus kann sich die Frage ergeben, ob durch die verpflichtende menschliche Aufsicht die Schutzwirkung der DSGVO teilweise umgangen wird (Sarra, 2025).

Hinzu kommen mögliche Spannungsverhältnisse zwischen Cybersicherheitsanforderungen und datenschutzrechtlichen Grundsätzen, wenn etwa personenbezogene Daten für eine Analyse von Cyberangriffen länger aufbewahrt werden sollen (Kelber, 2025).

Auch die föderale Struktur Deutschlands spielt eine Rolle: Die unterschiedlichen Auslegungen der DSGVO durch die 16 Landesdatenschutzbehörden können für Unternehmen mit bundesweiten Tätigkeiten zu erheblichen Unsicherheiten führen. So kann es zu widersprüchlichen Auslegungen kommen, was die grenzüberschreitende Konformität für KMU erschweren kann (Joswig/Kurz, 2025b).

3. Auswirkungen auf KMU – KI-Verordnung

Die europäische KI-Verordnung schafft erstmals einen einheitlichen Rechtsrahmen für die Entwicklung, Bereitstellung und Nutzung von KI-Systemen im Europäischen Wirtschaftsraum und verbindet den Anspruch, Grundrechte zu schützen, mit dem Ziel, Innovation zu fördern. Für KMU bedeutet das: Je nachdem, inwiefern sie KI-Systeme entwickeln, vertreiben oder einsetzen, unterscheiden sich die konkreten Pflichten und Gestaltungsspielräume. Chancen entstehen in jedem Fall.

Dieses Kapitel untersucht zunächst, welche Unternehmen in Deutschland voraussichtlich von der KI-Verordnung betroffen sind, und analysiert anschließend ihre Ausgangslage im Hinblick auf die Umsetzung der Vorgaben. Darauf aufbauend werden zentrale Herausforderungen, Kosten- und Nutzenaspekte sowie der daraus resultierende Unterstützungsbedarf für KMU herausgearbeitet.

3.1 Betroffenheitsanalyse

Grundsätzlich müssen alle KMU unabhängig von ihrer Unternehmensgröße, die KI entwickeln oder nutzen, selbst prüfen, ob sie unter die Regelungen der KI-Verordnung fallen. Entscheidend ist insbesondere die korrekte Einstufung des eingesetzten KI-Systems in eine der Risikoklassen der Verordnung, da sich daraus weitreichende Compliance-Pflichten ergeben können. Hinzu kommen Anforderungen, die unabhängig von der Risikoklassifizierung gelten. So müssen Arbeitgeber als Betreiber von KI-Systemen Maßnahmen ergreifen, damit die Beschäftigten über die notwendigen

Kompetenzen verfügen, um KI sachkundig einzusetzen und mögliche Risiken zu erkennen. Zwar sind diese Pflichten nicht bußgeldbewehrt, ihre Missachtung kann jedoch als Sorgfaltspflichtverletzung gelten und im Schadensfall eine Schadensersatzpflicht auslösen (BDA, 2024).

Für die Abschätzung des Kreises prüfungspflichtiger Unternehmen ist relevant, wie stark KI-Anwendungen im Unternehmensalltag verbreitet sind. Die verfügbaren Erhebungen unterscheiden sich nach Methodik (z. B. Befragungen vs. Webcrawling), Fokus (z. B. Technologieeinsatz vs. Kompetenzbedarf) und Zielgruppe (z. B. Unternehmen ab zehn Beschäftigten, bis 499 Beschäftigte).

Laut Erhebungen von Eurostat (2025) hat die Verwendung von KI in deutschen Unternehmen innerhalb eines Jahres deutlich zugenommen. Im Jahr 2024 setzten 18,8 Prozent der Unternehmen mit zehn bis 249 Beschäftigten mindestens eine KI-Technologie ein – fast doppelt so viele wie im Vorjahr. Einen großen Anteil daran haben die großen Sprachmodelle: Text Mining, Spracherkennung und Erzeugung natürlicher Sprache sind die am häufigsten genutzten Technologien, insbesondere in Marketing und Vertrieb. Große Unterschiede gibt es je nach Unternehmensgröße: Während 17 Prozent der Unternehmen mit zehn bis 49 Beschäftigten KI einsetzen, sind es in den Unternehmen mit 50 bis 249 Beschäftigten 28 Prozent und in den Unternehmen mit 250 und mehr Beschäftigten 48 Prozent. Größere Unternehmen setzen KI deutlich häufiger im Bereich IT-Sicherheit ein (ebd.).

Auf Basis des Unternehmensregisters, das rund 391.400 Unternehmen mit zehn bis 249 Beschäftigten erfasst (Statistisches Bundesamt, 2025), müssten unter der Annahme, dass knapp 19 Prozent der KMU KI einsetzen, deutschlandweit rund 73.500 dieser Unternehmen eine grundsätzliche Betroffenheitsprüfung im Hinblick auf die KI-Verordnung durchführen. Hinzu kommen fast 2,9 Millionen Kleinstunternehmen mit weniger als zehn Beschäftigten. Selbst wenn nur 3 Prozent von ihnen prüfungspflichtig wären, beträfe dies bereits rund 86.000 Unternehmen – je nach Branche dürfte der tatsächliche Anteil höher liegen.

Die regionale Verbreitung von KI im Mittelstand wird durch den von der IW Consult entwickelten Digitaler-Vorreiter-Index (DVI) abgebildet. Dieser nutzt Webcrawling, um den KI-Bezug von Unternehmen mit zehn bis 499 Beschäftigten zu erfassen und regional einzuordnen. Die Analyse zeigt eine deutliche Ballung der KI-Affinität in bestimmten Regionen (Abbildung 3-1).

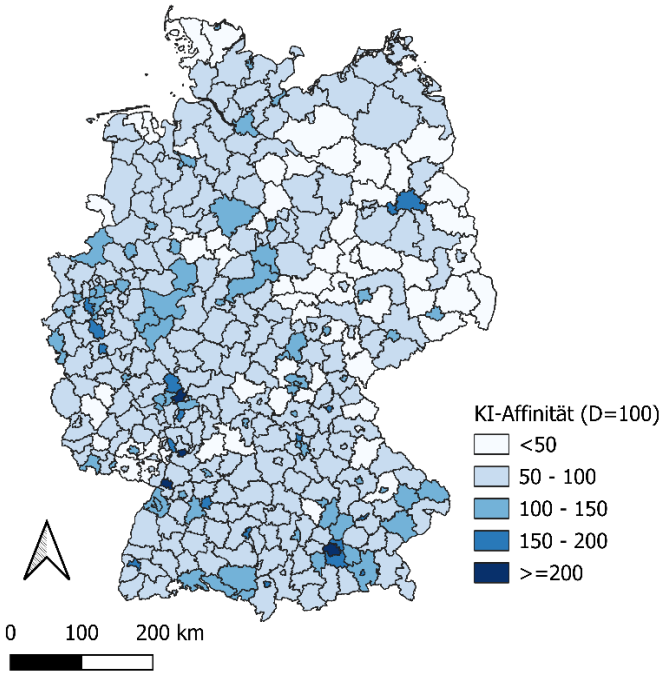
Besonders hoch ist die KI-Affinität des Mittelstands in der Stadt und im umgebenden Landkreis München sowie in den Städten Frankfurt am Main, Heidelberg, Karlsruhe, Darmstadt, Stuttgart, Bonn, Ulm und Potsdam. Hochschulstandorte sind dabei besonders stark vertreten – ein Hinweis auf mögliche Kooperationen zwischen Wissenschaft und Wirtschaft, aber auch auf die lokale Branchenstruktur. KI wird besonders häufig im Informations- und Kommunikationssektor sowie bei freiberuflichen, wissenschaftlichen und technischen Dienstleistungen eingesetzt, die häufiger in größeren Städten angesiedelt sind.

Weitere Studien zur regionalen Verteilung von KI-Stellenanzeigen in der Gesamtwirtschaft, auch im Hinblick auf generative KI, zeichnen ein ähnliches Bild. Auch hier liegt München an der Spitze (Büchel et al., 2025; Büchel/Engler, 2024). Eine spezifische Auswertung der KI-Stellenanzeigen für KMU ist im Rahmen der Begleitforschung von Mittelstand-Digital geplant.

Eine intensivere Betroffenheit von der KI-VO ergibt sich insbesondere dann, wenn Unternehmen KI-Systeme entwickeln oder nutzen, die in höhere Risikoklassen fallen. Die Mehrheit der KI-nutzenden KMU setzt derzeit vor allem kostenfreie, standardisierte Tools ein (Engels et al., 2025), die in der Regel den Risikoklassen „niedrig" oder „begrenzt" zugeordnet werden und daher nur geringfügig reguliert sind. Anders sieht es bei selbst entwickelten oder zugekauften KI-Verfahren aus: 13 Prozent der kleinen und 26 Prozent der mittleren Unternehmen setzen KI-Systeme ein, die von Dritten erworben wurden, während 4 Prozent der kleinen und 10 Prozent der mittleren Unternehmen eigene KI-Verfahren entwickeln (ebd.). In diesen Fällen ist eine individuelle Risikoklassifizierung erforderlich, die – je nach Ergebnis – umfangreiche regulatorische Pflichten wie

Risikomanagement oder technische Dokumentation auslösen kann. Bislang wird die KI-VO von jedem dritten Unternehmen als Hemmnis für den KI-Einsatz wahrgenommen (Scheufen et al., 2025).

Abbildung 3-1: KI-Affinität nach Kreisen



Index: Bundesweiter Durchschnitt aller Unternehmen (zehn bis 499 Beschäftigte) = 100 (Stand: Q2/2025)
Quelle: Eigene Berechnung IW Consult

3.2 Ausgangslage der betroffenen Unternehmen

Obwohl die KI-Verordnung bereits 2024 in Kraft getreten ist und erste Pflichten wie ein ausreichendes Maß an KI-Kompetenz bereits Anfang 2025 anwendbar geworden sind (siehe Abschnitt 2.1), haben sich bisher nur wenige Unternehmen intensiv mit den neuen Anforderungen auseinandergesetzt. So ist laut einer Bevölkerungsumfrage bisher lediglich ein Fünftel der Berufstätigen im Job zu KI geschult worden (Bitkom, 2025b). 70 Prozent der Berufstätigen geben an, keine KI-Fortbildungen vom Arbeitgeber angeboten bekommen zu haben (ebd.). Eine Umfrage unter Expertinnen und Experten zeigt, dass Unternehmen mit der DSGVO deutlich vertrauter als mit der KI-VO sind (Joswig/Kurz, 2025b).

Gleichzeitig verfügen viele KMU über stark begrenzte finanzielle und personelle Ressourcen, was die Umsetzung und Einhaltung der neuen Vorschriften erschwert. So bringen die Anforderungen der KI-Verordnung zusätzliche Belastungen mit sich, die die Innovationsfähigkeit der Unternehmen beeinträchtigen könnten (Davallas et al., 2025). Insbesondere binden Risiko- und Qualitätsmanagement, technische Dokumentation und Daten-Governance sowie Konformitätsbewertungen und die fortlaufende Überwachung des Systems nach Markteinführung erhebliche Entwickler- und Compliance-Ressourcen. Das verlängert die Zeit vom Entwicklungsstart bis zur Markteinführung (Time-to-Market), erhöht Fixkosten und verdrängt Experimente in frühen Prototypphasen.

Angesichts der hohen Dynamik, mit der sich der Einsatz von KI in den Unternehmen verbreitet (siehe Abschnitt 3.1), ist es für KMU umso dringlicher, sich frühzeitig mit den Anforderungen der KI-VO zu befassen. Denn die Umsetzung erfordert, sich einer Reihe komplexer Herausforderungen zu stellen.

3.3 Zentrale Herausforderungen im Kontext der KI-Verordnung

Für KMU ist die KI-Verordnung mit Neuerungen verbunden. Sobald sie KI-Systeme entwickeln oder einsetzen, müssen sie Compliance-Anforderungen erfüllen – denn einige Pflichten gelten unabhängig von der Risikoklassifizierung. So verlangt die Verordnung von Anbietern und Betreibern von KI-Systemen (siehe Abschnitt 2.1), Maßnahmen zu ergreifen, um sicherzustellen, dass ihr Personal über ausreichende KI-Kompetenzen verfügt. Schulungen sind dabei auf technische Kenntnisse, Erfahrung, Ausbildung und den konkreten Einsatzkontext abzustimmen. Auch Transparenzpflichten können unabhängig von der Risikoklasse greifen, etwa bei KI-Systemen, die für die direkte Interaktion mit Menschen bestimmt sind. In diesen Fällen ist klarzustellen, dass es sich um ein KI-System handelt oder die Ausgabe KI-generiert ist.

Deutlich komplexer werden die Anforderungen beim Einsatz von Hochrisiko-KI-Systemen (siehe Abschnitt 2.1). Hier ist die Risikoklassifizierung von zentraler Bedeutung – und für viele KMU zugleich eine große Hürde. Es ist zu erwarten, dass zahlreiche Unternehmen ihre Systeme nicht sicher einer Risikoklasse zuordnen können. Die Folge sind betriebliche Risiken (Joswig/Kurz, 2025b), verschärft durch die Komplexität der Vorschriften, welche eine korrekte Interpretation erschwert. Hinzu kommt, dass KI-Ökosysteme häufig arbeitsteilig organisiert sind, was bei den komplexen Anforderungen an Hochrisiko-KI-Systeme die Verantwortlichkeiten und regulatorischen Zuständigkeiten in der Wertschöpfungskette schwer durchschaubar macht (Kajava et al., 2025). Für KMU mit begrenzten personellen und finanziellen Ressourcen wiegt dies besonders schwer.

Eine weitere Herausforderung für KMU liegt in den bestehenden Rechtsunsicherheiten bei der Umsetzung der KI-Verordnung. Sie ergibt sich aus unklaren Begriffen in der Verordnung, die nach Einschätzung des BDI (2025) auch risikoarme Anwendungen erfassen können. Verstärkt werden die Unsicherheiten durch das Zusammenspiel mit anderen Regelwerken wie NIS-2, CRA und DSGVO (siehe Abschnitt 2.4). Da viele Fragen erst durch künftige Rechtsprechung geklärt werden, müssen Unternehmen Entwicklungen kontinuierlich beobachten und ihre Prozesse gegebenenfalls anpassen.

Eine besondere Herausforderung für KMU könnte sich aus dem Wechselspiel mit der DSGVO ergeben. So ist die gleichzeitige Einhaltung von DSGVO und KI-VO für viele KMU aufgrund beschränkter finanzieller und personeller Mittel kaum zu bewältigen. Dies gilt insbesondere bei Hochrisiko-Anwendungen, die hohe Anforderungen an Transparenz, Dokumentation und menschliche Kontrolle stellen (Joswig/Kurz, 2025b).

Bei allen Maßnahmen müssen Unternehmen den gestaffelten Zeitplan der KI-VO im Blick behalten, um rechtzeitig vor Inkrafttreten der jeweiligen Pflichten handlungsfähig zu sein.

3.4 Kosten im Kontext der KI-Verordnung

Die Umsetzung der KI-Verordnung bringt für betroffene Unternehmen – insbesondere KMU – spürbare Kosten mit sich. Viele befürchten, dass die hohen Anforderungen die globale Wettbewerbsfähigkeit der EU-Unternehmen beeinträchtigen, vor allem bei begrenzten Ressourcen (Kajava et al., 2025).

In ihrem Impact Assessment hat die Europäische Kommission (2021) die Auswirkungen der KI-Verordnung auf Unternehmen untersucht und dabei potenzielle Belastungen für die Wettbewerbsfähigkeit und das Innovationspotenzial von KMU identifiziert. Bei Hochrisiko-KI-Systemen müssen KMU dieselben umfangreichen Pflichten erfüllen wie große Unternehmen, etwa Risikomanagement, technische Dokumentation und Konformitätsbewertungen. Diese Vorgaben können für KMU überproportional belastend sein. Die Kommission hält ihre Einbeziehung dennoch für gerechtfertigt, da auch von KMU entwickelte KI-Systeme erhebliche gesellschaftliche Relevanz entfalten können.

Die Kostenabschätzung ist umstritten, da sie stark von methodischen Annahmen abhängt (Laurer et al., 2021). Mueller (2021) prognostiziert für die europäische Wirtschaft Gesamtlasten von rund

31 Milliarden Euro über fünf Jahre, was nach seiner Ansicht zu einem Rückgang der KI-Investitionen um 20 Prozent führen könnte. Für ein KMU, das ein Hochrisiko-KI-System betreibt, veranschlagt Mueller bis zu 400.000 Euro an Gesamtkosten. Laurer et al. widersprechen dieser Berechnung, da Mueller unterstelle, alle KI-Systeme fielen unter die Hochrisiko-Regeln. Tatsächlich dürften laut Laurer et al. (2021) nur rund 10 Prozent aller KI-Investitionen von den schärferen Auflagen erfasst werden. Das Impact Assessment der Europäischen Kommission kommt zu einer ähnlichen Einschätzung: Nur 5 bis 10 Prozent der KI-Systeme gelten als Hochrisiko-Anwendungen (Europäische Kommission, 2021). Wenn ein KMU erstmals ein Qualitätsmanagementsystem für ein Hochrisiko-KI-System aufbauen muss, rechnen Laurer et al. (2021) mit einmaligen Kosten von 193.000 bis 330.000 Euro, zuzüglich laufender Wartungskosten von 71.400 Euro pro Jahr. Wird dieses Qualitätsmanagementsystem anschließend für mehrere KI-Systeme desselben Unternehmens genutzt, sinken die zusätzlichen Kosten je weiteres System deutlich: Im Mittel lägen die durchschnittlichen Gesamtkosten je System damit weit unter den von Mueller genannten 400.000 Euro.

Haataja und Bryson (2021) unterscheiden in ihrer Schätzung zwischen Anbietern und Betreibern sowie zwischen Compliance- und Konformitätsbewertungskosten. Sie gehen bei einem KI-Entwicklungspreis von ca. 170.000 Euro von jährlichen Compliance-Kosten zwischen 5.000 und 8.000 Euro sowie einmaligen Kosten von 3.000 bis 7.500 Euro für die Konformitätsbescheinigung aus. Insgesamt könnten die Regulierungskosten also bis zu 10 Prozent der Entwicklungskosten betragen.

Festzuhalten bleibt: Die meisten KI-Systeme verursachen keine oder nur geringfügige Regulierungskosten. Ein kleiner Teil der KI-Systeme, vor allem Hochrisiko-Anwendungen, verursacht erheblichere Regulierungskosten. Bei individueller Betroffenheit können die Kosten schnell einen substanziellen Anteil der jeweiligen KI-Investition ausmachen, was KMU durchaus von der Entwicklung oder Nutzung solcher Systeme abhalten könnte.

Um Überlastungen zu vermeiden, hat die Kommission im Impact Assessment gezielte Entlastungen vorgeschlagen, darunter regulatorische Sandkästen[6] zur erleichterten Testung innovativer Systeme sowie gestaffelte Gebührenmodelle für Konformitätsbewertungen, angepasst an die Unternehmensgröße (Europäische Kommission, 2021). Diese KMU-spezifischen Erleichterungen wurden im Gesetzgebungsverfahren aufgenommen. Details zur Umsetzung finden sich in Abschnitt 3.6.

3.5 Nutzen der KI-Verordnung

Neben den mitunter hohen Umstellungskosten birgt die KI-Verordnung auch konkrete Chancen für Unternehmen – insbesondere für KMU. Das Impact Assessment der Europäischen Kommission (2021) identifiziert zentrale Nutzenaspekte, die langfristig Wettbewerbsvorteile schaffen können:

- Vertrauensbildung: Die KI-Verordnung soll das Vertrauen in den Einsatz von KI stärken. Davon profitieren insbesondere KMU, die KI-Systeme anbieten, da sie in der Regel weniger bekannt sind und sich nicht wie große Unternehmen auf ein etabliertes Markenimage stützen können. Eine regulatorisch abgesicherte Vertrauensbasis erleichtert ihnen den Marktzugang.
- Verbesserter Marktzugang durch Harmonisierung: Eine einheitliche EU-Regulierung verhindert eine regulatorische Fragmentierung und senkt Markteintrittsbarrieren. Während große Unternehmen nationale Unterschiede leichter überbrücken können, profitieren KMU besonders von der Vereinheitlichung.

[6] Regulatorische Sandkästen – auch Reallabore genannt – sind rechtliche Rahmenbedingungen auf Basis von Experimentierklauseln. Sie ermöglichen es, innovative Technologien, Produkte, Dienstleistungen oder Ansätze in einer realen Umgebung und für einen begrenzten Zeitraum bzw. in einem abgegrenzten Sektor oder Gebiet unter regulatorischer Aufsicht zu erproben, wobei zugleich angemessene Schutzmaßnahmen gewährleistet werden (Rat der Europäischen Union, 2020).

- Kostenvorteile durch Standardisierung: Harmonisierte Standards reduzieren den Entwicklungsaufwand und ermöglichen es, einmal entwickelte Lösungen in mehreren EU-Staaten ohne große Anpassungen einzusetzen.
- Verringerung rechtlicher Unsicherheit: Einheitliche Vorschriften schaffen Klarheit, was gerade KMU ohne ausgeprägte rechtliche Expertise zugutekommt.

Gleichzeitig zeigen Unternehmensbefragungen ein ambivalentes Bild. In einer Deloitte-Umfrage (2024) unter 500 privatwirtschaftlichen Entscheidern in Deutschland, die bereits von der KI-Verordnung gehört haben, erwartet die Mehrheit negative Auswirkungen auf Innovationsmöglichkeiten, nur knapp ein Fünftel sieht positive Effekte. Unternehmen begründen dies damit, dass Regulierung oft kurzfristig bremst, langfristig jedoch für einen stabileren Rahmen sorgt. Auch in einer repräsentativen Bitkom-Umfrage (2024) befürchten 45 Prozent der Unternehmen ab 20 Beschäftigten, dass die KI-Verordnung die Entwicklung von KI in Europa hemmen wird. In einem Impulspapier wird aufgezeigt, dass in der Medizintechnik KMU und Start-ups durch die KI-Verordnung aufgrund fehlender personeller Ressourcen vor Herausforderungen durch zusätzliche Pflichten stehen, was sich negativ auf die Innovationsfähigkeit auswirken könnte. Gleichzeitig werden im Impulspapier Vorschläge gemacht, wie die KMU unterstützt werden könnten, etwa durch branchenspezifischer Muster als Vorlagen für regulatorische Prozesse (Budde et al., 2025).

Das Vertrauen in KI ist derzeit gering: Laut einer bevölkerungsrepräsentativen Befragung (SAS, 2024) fühlen sich 80 Prozent unwohl bei automatisierten, nicht von Menschen kontrollierten KI-Entscheidungen in der Personalauswahl; 69 Prozent äußern dasselbe Unbehagen bei Bank- und Versicherungsentscheidungen. In der Deloitte-Befragung (2024) glauben 35 Prozent der Unternehmen, dass die KI-Verordnung zu mehr Vertrauen führen wird, während 31 Prozent dies verneinen. Sicherheitsbedenken spielen – neben Faktoren wie Nützlichkeit und Benutzerfreundlichkeit (Sanchez-Holgaldo/Arcila-Calderón, 2024) – eine wesentliche Rolle bei der Akzeptanz von KI-Anwendungen in Wirtschaft und Gesellschaft (Rane et al., 2024). Eine Befragung aus dem Jahr 2025 zeigt, dass 66 Prozent der Befragten Datenschutzbedenken haben und den Missbrauch persönlicher Daten durch KI-Systeme befürchten (Ganser/Reich, 2025).

Trotz der vorhandenen Skepsis kann die Verordnung mittel- bis langfristig Vertrauen schaffen, da sie differenziert nach Risikoklassen reguliert und damit gezielt auf unterschiedliche Anwendungskontexte eingeht (Tamó-Larrieux et al., 2023). Kurzfristig bestehen allerdings Rechtsunsicherheiten wegen unklaren Verordnungsbegriffen und Abgrenzungen; viele KMU wissen zudem nicht, ob und in welchem Umfang sie betroffen sind. Der scheinbare Widerspruch lässt sich so auflösen: Derzeit erzeugt die Einführung noch Auslegungsfragen, während nach Präzisierung durch Leitfäden, harmonisierte Normen und eine vorhersehbare Aufsichtspraxis die Verordnung vor allem auch auf der Nutzendenseite Rechtssicherheit erhöht, Unsicherheiten abbaut und Vertrauen fördert. Deloitte (2024) berichtet, dass 40 Prozent der Unternehmen mehr Rechtssicherheit erwarten, 35 Prozent keine Verbesserung sehen und 25 Prozent unentschlossen sind. Bitkom (2024) meldet dagegen, dass 60 Prozent eine erhöhte Rechtssicherheit bei Entwicklung und Einsatz von KI erwarten.

Ohne einen klaren Rechtsrahmen müssten Unternehmen Vertrauenswürdigkeit eigenständig herstellen – etwa durch Selbstverpflichtungen, Transparenzmaßnahmen oder (teilweise noch zu entwickelnde) Zertifizierungen – was gerade für KMU kosten- und ressourcenintensiv wäre. Vor dem Hintergrund der Kosten-Nutzen-Abwägung ist die KI-Verordnung daher nicht zwingend als zentrales Hemmnis für den KI-Einsatz zu sehen: Laut Scheufen et al. (2025) betrachten 32 Prozent der deutschen Unternehmen sie als Hemmnis, während 40 Prozent den Datenschutz als Hürde einstufen.

3.6 Unterstützungsbedarfe der KMU

Vor dem Hintergrund der in den vorangegangenen Abschnitten dargestellten Herausforderungen, Kosten und Nutzen der KI-Verordnung ergeben sich für KMU spezifische Unterstützungsbedarfe.

So geben denn auch 69 Prozent der Unternehmen in Deutschland an, Unterstützung bei der Umsetzung zu benötigen (Bitkom, 2024a). Die Unterstützungsbedarfe der KMU können drei zentralen Dimensionen zugeordnet werden:

- Informationsbedarf: Viele KMU verfügen bislang nur über begrenztes Wissen zu den konkreten Inhalten der KI-Verordnung. Unklar bleibt oft, ob sie überhaupt von den Regelungen betroffen sind, wie ihre KI-Systeme rechtlich einzustufen sind und welche Pflichten sich daraus ableiten. Da die Rechtslage dynamisch ist und sich durch neue EU-Durchführungsrechtsakte, nationale Umsetzungsgesetze und gerichtliche Entscheidungen weiterentwickelt, reicht eine einmalige Information nicht aus. KMU benötigen daher kontinuierlich aktuelle, verständlich aufbereitete und rechtlich belastbare Informationen, um ihre Entscheidungen auf einer sicheren Grundlage treffen zu können.
- Kompetenzbedarf: Die Umsetzung der KI-Verordnung erfordert spezifisches Fachwissen – sowohl im technischen als auch im rechtlichen Bereich. Insbesondere die Anforderungen an Risikomanagement, technische Dokumentation, Konformitätsbewertung und Transparenzmaßnahmen setzen Kenntnisse voraus, die in vielen KMU nicht vorhanden sind (Ferner, 2024). Daher besteht ein hoher Bedarf an praxisnahen Schulungen, Workshops und Begleitung von KI-Umsetzungsprojekten, die auf die spezifischen Anwendungsfälle von KMU zugeschnitten sind und den Wissenstransfer zwischen Recht, Technik und Management ermöglichen.
- Ressourcenbedarf: Neben Wissen und Kompetenzen benötigen KMU auch ausreichende personelle und finanzielle Ressourcen, um die Umsetzung der KI-Verordnung stemmen zu können. Viele kleinere Unternehmen verfügen weder über eine eigene Rechtsabteilung noch über dedizierte Compliance-Teams (Eger/Scheufen, 2024; Demary et al., 2025). Die kontinuierliche Beobachtung regulatorischer Entwicklungen, die Anpassung interner Prozesse und die Durchführung notwendiger Prüf- und Zertifizierungsverfahren binden erhebliche Kapazitäten. Externe Dienstleistungen können hier entlasten, verursachen jedoch zusätzliche Kosten. Deshalb sind Maßnahmen nötig, die KMU den Zugang zu kostengünstigen oder geförderten Unterstützungsleistungen erleichtern.

Die KI-Verordnung sieht bereits spezifische Entlastungen für KMU vor, darunter regulatorische Sandkästen, geringere Gebühren für die Konformitätsbewertung sowie vereinfachte Dokumentations- und Schulungspflichten. Diese Erleichterungen sind jedoch bislang nicht umgesetzt. Auf europäischer Ebene stehen noch Durchführungsrechtsakte aus, die die Rahmenbedingungen für regulatorische Sandkästen festlegen. Der KI-Service Desk der Bundesnetzagentur (2025) informiert fortlaufend über den Stand dieser Rechtsakte und deren Bedeutung für die Praxis. Sollten die Regelungen in Kraft treten, bevor die Unterstützungsstrukturen etabliert sind, wären KMU zunächst auf teure externe Zertifizierungen angewiesen (BDI, 2024). Um unnötige Belastungen zu vermeiden, ist eine zügige Umsetzung der entlastenden Elemente notwendig.

3.6.1 Bestehende Unterstützungsangebote

Vielen KMU ist die KI-Verordnung bislang noch nicht bekannt, obwohl ihre Regelungen bereits teilweise in Kraft sind. Um das zu ändern, sind zielgerichtete Informations- und Unterstützungsangebote entscheidend.

Eine zentrale Rolle spielen dabei die vom Bundesministerium für Wirtschaft und Energie geförderten Mittelstand-Digital Zentren (MDZ). Sie bieten Blogbeiträge, Fachartikel, kompakte Übersichten und Checklisten, die speziell auf KMU zugeschnitten sind. Darüber hinaus unterstützen sie Unternehmen bei der Identifikation von KI-Systemen im Betrieb, der Einstufung in Risikoklassen sowie der Erstellung individueller Pflichtenkataloge (z. B. MDZ Chemnitz, 2025; MDZ Berlin, 2025). Die Online-Formate der MDZ reichen von kurzen Einstiegsangeboten wie „EU AI Act kompakt“ (MDZ Rostock) oder „Pflicht zur KI-Kompetenz – Was der EU-AI-Act von Unternehmen fordert“ (MDZ

Lingen.Münster.Osnabrück) über rechtliche Informationen zu verschiedenen KI-Aspekten (Wissensbox Recht des MDZ Chemnitz) bis zu vertiefenden 3,5-Stunden-Workshops wie „Smart auf der sicheren Seite – KI rechtssicher nutzen" (MDZ Chemnitz).

Neben den themen- oder branchenbezogenen oder regionalen MDZ bieten auch andere Anlaufstellen den KMU Informationen zur Digitalisierung, wie die European Digital Innovation Hubs (EDIHs), die Industrie- und Handelskammern, Handwerkskammern, Wirtschaftsförderungen, Digitalagenturen, Branchenverbände oder Unternehmensnetzwerke (Ramboll, 2024). Zu deren Angeboten gehören auch Workshops, Webinare, E-Learning-Formate und Veranstaltungen zur KI-Verordnung (z. B. IHK Köln, 2025).

Ergänzend unterstützen die vom Bundesministerium für Arbeit und Soziales und dem Europäischen Sozialfonds Plus geförderten Zukunftszentren Unternehmen dabei, KI-Anwendungen einzuführen und die dafür nötigen Kompetenzen im Betrieb aufzubauen. Sie bieten Workshops, Lernlabore und Qualifizierungen zu KI-Nutzung, Veränderungsprozessen und Mitarbeitendenbeteiligung. Beispielhaft begleitet das hessische Zukunftszentrum ZUKIPRO Produktionsbetriebe bei der Einführung von KI-Lösungen und Schulungen zu AI Literacy (ZUKIPRO, 2025).

Ein umfassendes Informationsangebot zur KI-Verordnung bietet die Bundesnetzagentur seit Juli 2025. Das KI-Service Desk unterstützt Unternehmen beispielsweise durch den KI-Compliance Kompass bei der Umsetzung der Verordnung (Bundesnetzagentur, 2025). Die Bundesnetzagentur stellt zudem Informationen über die bereits geltende Verpflichtung bereit, dass Mitarbeitende, die mit KI-Systemen arbeiten, über eine angemessene KI-Kompetenz (AI Literacy) verfügen müssen. Der KI-Service Desk bietet hierzu kostenfreie Weiterbildungsangebote und praxisnahe Orientierungshilfen für Unternehmen.

Auch die Datenschutzkonferenz (2025) hat mit ihrer „Orientierungshilfe zu empfohlenen technischen und organisatorischen Maßnahmen bei der Entwicklung und beim Betrieb von KI-Systemen" erste Hilfestellungen veröffentlicht. Verschiedene weitere Angebote unterstützen Unternehmen ebenfalls auf technischer oder strategischer Ebene – etwa der AI Act Risk Navigator vom TÜV AI.Lab (https://www.tuev-risk-navigator.ai/), der erste Anhaltspunkte zur Risikoklassifizierung liefert, oder der Bavarian AI Act Accelerator des Bayerischen Staatsministeriums für Digitales (2025). Auch die IHK München und Oberbayern (2025) stellt Informationsmaterial zur Verfügung. Dennoch fehlt es bislang an einer systematischen Übersicht, die die Vielzahl der Regelungen verständlich aufbereitet, deren Wechselwirkungen berücksichtigt und unterschiedliche Anwendungsfälle praxisnah abbildet.

Auch die in der KI-Verordnung vorgesehenen entlastenden Elemente für KMU befinden sich noch in der Aufbauphase. Die EU-Mitgliedstaaten sollen bis zum 2. August 2026 nationale KI-Reallabore einrichten. Bestehende deutsche Initiativen – wie das Pilotprojekt eines KI-Reallabors der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, des Landes Hessen und der Bundesnetzagentur (BfDI, 2025) – erfüllen bislang nicht den formalen Status eines regulatorischen Sandkastens im Sinne der Verordnung. Ergänzend dazu existieren Initiativen wie der AI Quality & Testing Hub des Landes Hessen und des Verbands der Elektrotechnik Elektronik und Informationstechnik (VDE) (https://aiqualityhub.com/), die kostenlose Beratung und der freiwillige Qualitätsstandard des IQZ Kaiserslautern (Mission KI) oder die SmartFactoryOWL als offene Datenplattform für KI-Anwendungen in der Industrie 4.0 (https://smartfactory-owl.de/ki-reallabor/).

Auf europäischer Ebene unterstützt das Projekt „EU Regulatory Sandboxes for AI" die Mitgliedstaaten beim Aufbau nationaler regulatorischer Sandkästen und fördert den Wissensaustausch. Ergänzend entstehen sektorspezifische Testing and Experimentation Facilities (TEFs), die KI-Technologien unter realen Bedingungen erproben – bisher in den Bereichen Agrar- und Lebensmittelwirtschaft, Gesundheitswesen, industrielle Fertigung sowie intelligente Städte und Gemeinden (Europäische Kommission, 2025b). Das European High-Performance Computing Joint Undertaking (EuroHPC JU) baut europaweit sogenannte KI-Fabriken (AI Factories) auf. In Deutschland entstehen zwei Standorte in Stuttgart und Jülich. Die KI-Fabriken dienen als zentrale Anlaufstellen für

KI-Start-ups, KMUs und Forschende. In Jülich umfasst die KI-Fabrik neben dem Exascale-Supercomputer JUPITER auch JARVIS als experimentelle Plattform für die Entwicklung und Erprobung innovativer KI-Modelle und -Anwendungen (Europäische Kommission, 2025c).

3.6.2 Empfehlungen zur Weiterentwicklung

Vor dem Hintergrund der identifizierten Herausforderungen und Unterstützungsbedarfe sowie der Analyse bestehender Angebote lassen sich für die Weiterentwicklung der Unterstützungsstruktur für KMU im Kontext der KI-Verordnung folgende Handlungsprioritäten ableiten:

- Zentrale Plattform einrichten: Es sollte eine gut sichtbare, einheitliche Informationsplattform geschaffen werden, auf der alle relevanten Angebote, Schulungen, rechtlichen Hinweise und praxisnahen Hilfsmittel zur KI-Verordnung gebündelt sind. Diese Plattform sollte auch den Zugang zu künftigen Unterstützungsmaßnahmen wie den geplanten regulatorischen Sandkästen ermöglichen. Der KI-Service Desk der Bundesnetzagentur (2025) markiert hierfür einen ersten Schritt.
- Branchenspezifische Differenzierung ausbauen: Die bestehenden Unterstützungsangebote sollten stärker nach Branchen und Anwendungsbereichen differenziert werden, um den unterschiedlichen regulatorischen Anforderungen gerecht zu werden. So gelten für KI-Systeme in der medizinischen Diagnostik andere Voraussetzungen als für KI in der industriellen Prozessoptimierung. Sektorspezifische Leitlinien, Musterverträge oder branchenspezifische Schulungsangebote könnten hier entscheidend dazu beitragen, bestehende Hemmnisse abzubauen und den rechtssicheren KI-Einsatz zu erleichtern (Demary et al., 2025).
- Rechtsentwicklung systematisch beobachten: Eine zentrale Monitoring-Stelle könnte kontinuierlich neue EU- und nationale Regelungen, Gerichtsentscheidungen und interpretierende Dokumente erfassen, bewerten und für KMU verständlich aufbereiten.
- Entlastungsmaßnahmen frühzeitig umsetzen: Die in der KI-Verordnung vorgesehenen Erleichterungen für KMU – wie vereinfachte Dokumentationspflichten, vergünstigte Konformitätsbewertungen oder regulatorische Sandkästen – sollten zügig implementiert werden, um Unternehmen rechtzeitig vor Inkrafttreten der verbindlichen Pflichten zu entlasten.

Damit können KMU baldmöglichst Sicherheit in der Anwendung der KI-Verordnung gewinnen, ihre Ressourcen gezielter einsetzen und regulatorische Risiken minimieren. Eine schnelle, koordinierte Umsetzung dieser Maßnahmen ist entscheidend, nicht nur um Compliance zu gewährleisten, sondern auch um die Innovationsfähigkeit des Mittelstands zu sichern und die Wettbewerbsposition europäischer Unternehmen im Bereich KI zu stärken.

4. Auswirkungen auf KMU – Cybersicherheitsregulierung

Neben der KI-Verordnung stellt auch die europäische Cybersicherheitsregulierung KMU vor neue Herausforderungen. Dieses Kapitel beleuchtet zunächst die Cybersicherheitslage kleiner und mittlerer Unternehmen, und analysiert anschließend Betroffenheit, Ausgangslage, Herausforderungen, Kosten und Nutzen im Kontext der NIS-2-Richtlinie sowie des Cyber Resilience Act. Im Anschluss wird das Zusammenspiel beider Regulierungen betrachtet. Darauf aufbauend werden bestehende Unterstützungsangebote analysiert und Empfehlungen für deren Weiterentwicklung abgeleitet.

4.1 Cybersicherheitslage in KMU

Zur Einschätzung der Cybersicherheitslage in KMU in Deutschland werden zwei komplementäre Indikatoren verwendet: das Cybersicherheitsrating und das inhärente Cyberrisiko. Die zugrunde liegenden Daten stammen von BitSight Technologies, Inc. und wurden über die Unternehmensdatenbank Orbis Europe von Moody’s Analytics bereitgestellt. Für die Analyse stehen Datensätze zu 17.578 Unternehmen mit 50 bis 250 Beschäftigten aus Deutschland zur Verfügung (Stand: Juli 2025). Die Veröffentlichung erfolgt mit Genehmigung von BitSight.

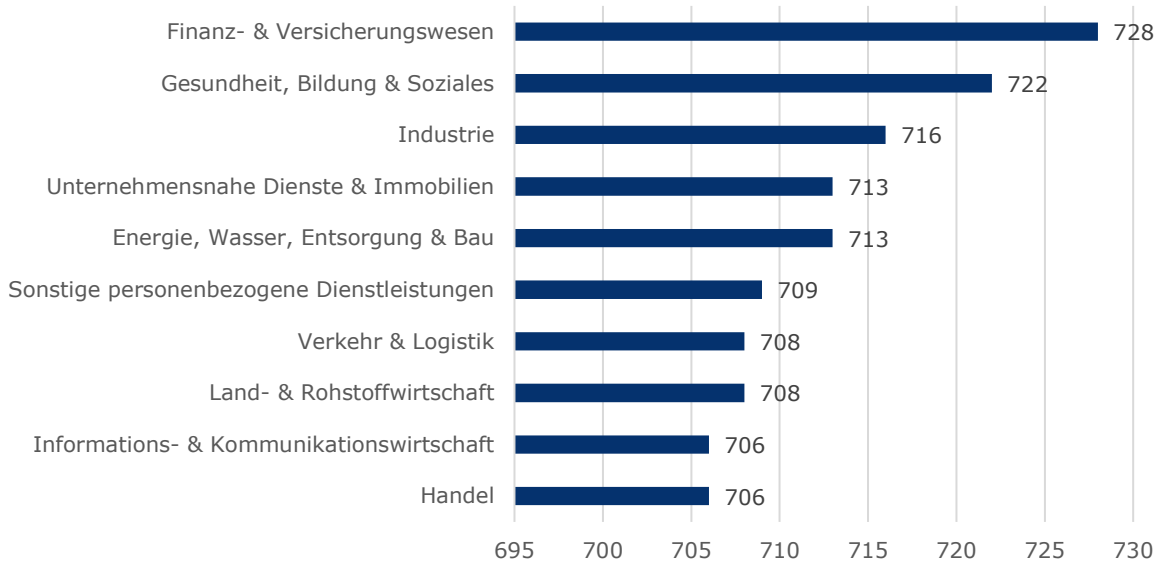
Das Cybersicherheitsrating bewertet die Sicherheitsleistung eines Unternehmens anhand extern beobachtbarer technischer Merkmale. Es berücksichtigt Risikovektoren in vier Dimensionen:

- Sicherheitsstandards: technische Sicherheitsstandards und -konfigurationen (auch „Diligence"), z. B. offene Netzwerkports, über die Angreifer auf Systeme zugreifen könnten, veraltete Verschlüsselungstechnologien, E-Mail-Schutzmechanismen
- Kompromittierte Systeme: aktive Sicherheitslücken und Schadaktivitäten im Unternehmenswerk, z. B. Botnet-Infektionen (Computer, die unbemerkt Teil eines Schadnetzwerks geworden sind), Schadsoftware, Spamversand
- Nutzendenverhalten: Nutzung unsicherer Netzwerke, riskante Datenfreigaben
- Sicherheitsvorfälle: öffentlich gewordene Datenlecks oder Ransomware-Angriffe

Methodisch entsteht das Rating zweistufig. Zunächst wird je Risikovektor aus den beobachteten Merkmalen ein roher Score berechnet, der unternehmensgrößenbereinigt und anschließend als Perzentil gegen die Gesamtheit aller weltweit bewerteten Organisationen eingeordnet wird. So erhält der Vektor seine Note relativ zur Population und bleibt auch bei Datenschwankungen vergleichbar stabil. Aus den angepassten Vektorwerten wird ein gewichteter Gesamtscore, das Cybersicherheitsrating, gebildet, der von BitSight regelmäßig normalisiert wird, um die angestrebte Verteilung auf der Skala 250–900 zu erzielen. Die Bewertung des Ratings reicht von 250 (niedrig) bis 900 (hoch) Punkten und wird in drei Kategorien eingeteilt: grundlegend (250–639), mittel (640–739) und fortgeschritten (740–900).

Die Analyse zeigt, dass die deutschen KMU im Durchschnitt ein mittleres Sicherheitsniveau erreichen: Die Bewertungen liegen branchenübergreifend zwischen 706 und 728 Punkten (Abbildung 4-1).

Abbildung 4-1: Cybersicherheitsrating nach Branchengruppen



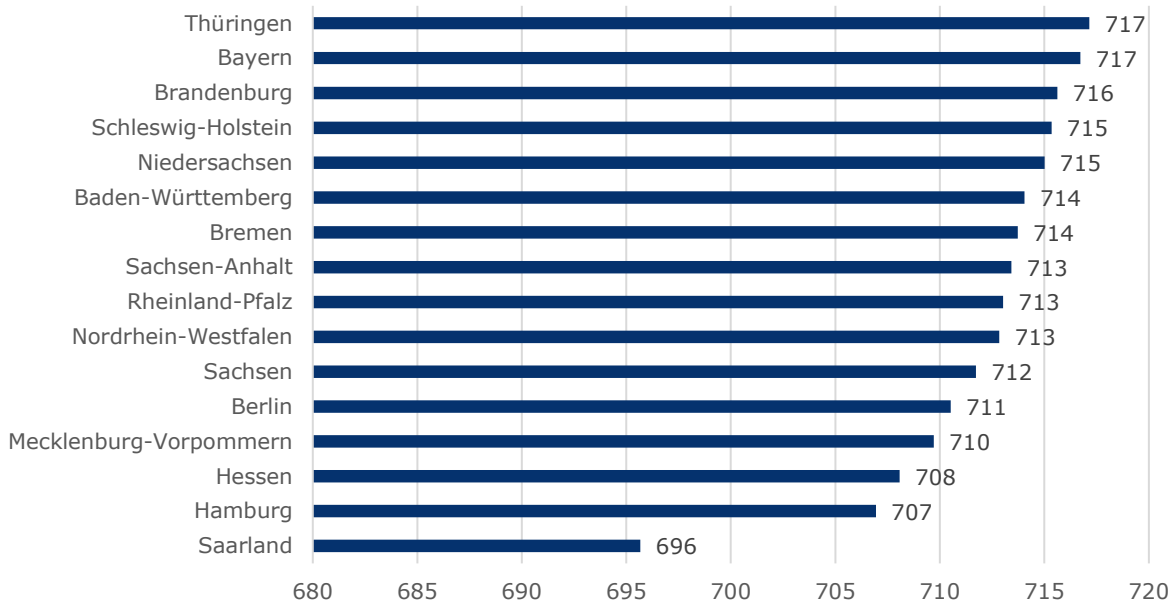
Cybersicherheitsniveau nach Branchengruppen (Durchschnitt von Juni 2024 bis Juli 2025); Einstufung: grundlegend (250-639), mittel (640-739), fortgeschritten (740-900); Unternehmen mit 50 bis 250 Beschäftigten.
Quelle: Eigene Berechnungen auf Basis von Daten der BitSight Technologies, Inc., bereitgestellt durch Moody's Analytics, Stand: Juli 2025 (n = 17.578). Veröffentlichung mit Genehmigung von BitSight.

Die höchsten Werte erreichen Finanz- und Versicherungsunternehmen sowie Organisationen aus Gesundheit, Bildung und Soziales. Am unteren Ende rangieren Handel sowie die Informations- und Kommunikationswirtschaft – allerdings ebenfalls im mittleren Bereich. Die Monatsergebnisse von Juni 2024 bis Juni 2025 zeigen keine signifikante Verbesserung über die Zeit. Vor dem Hintergrund der EU-Cybersicherheitsregulierung mag dies auf den ersten Blick überraschen. Allerdings

fehlt es in Deutschland weiterhin an einer nationalen Umsetzung der NIS-2-Richtlinie (Stand: Oktober 2025). Verbindliche Vorgaben, welche konkreten Sicherheitsmaßnahmen Unternehmen zu ergreifen haben, bestehen daher noch nicht. Dass sich im untersuchten Zeitraum bislang keine deutliche Verbesserung abzeichnet, ist daher weniger Ausdruck fehlender Relevanz, sondern eher ein Hinweis auf die regulatorische Zwischenphase und die begrenzten Ressourcen vieler KMU.

Regionale Unterschiede fallen moderat aus. Abbildung 4-2 zeigt: Die höchsten Ratings erzielen Thüringen und Bayern (717 Punkte), das Saarland ist mit 696 Punkten Schlusslicht. Damit liegen alle Bundesländer ebenfalls im mittleren Bereich. Ob die Differenzen auf regionale Unterstützungsangebote zurückzuführen sind, lässt sich nicht abschließend bewerten.

Abbildung 4-2: Cybersicherheitsrating nach Bundesländern



Cybersicherheitsniveau nach Bundesländern (Durchschnitt von Juni 2024 bis Juli 2025); Einstufung: grundlegend (250-639), mittel (640-739), fortgeschritten (740-900); Unternehmen mit 50 bis 250 Beschäftigten

Quelle: Eigene Berechnungen auf Basis von Daten der BitSight Technologies, Inc., bereitgestellt durch Moody's Analytics, Stand: Juli 2025 (n = 17.083). Veröffentlichung mit Genehmigung von BitSight.

Neben der beobachtbaren Cybersicherheitsperformance liefert das inhärente Cyberrisiko einen ergänzenden Blick auf die strukturelle Verwundbarkeit von KMU unabhängig von konkreten Schutzmaßnahmen. Es beruht auf unternehmensspezifischen Merkmalen – insbesondere Branche, Größe und Land – und erfasst, wie stark Unternehmen aufgrund ihrer typischen Risikofaktoren einem Cybervorfall ausgesetzt sind. Die Risikobewertung erfolgt relativ zur Referenzgruppe: Unternehmen mit sehr hohem Risiko (Wert 5) haben im Durchschnitt eine 10,9-fach höhere Wahrscheinlichkeit, von einem Vorfall betroffen zu sein, als Unternehmen mit sehr geringem Risiko (Wert 1). Besonders gefährdete KMU in Deutschland kommen aus den Bereichen Gesundheit, Bildung & Soziales (Durchschnittswert 3,9), Finanz- & Versicherungswesen (3,8) sowie Verkehr & Logistik (3,7) (Tabelle 4-1).

Diese Branchen sind zumindest teilweise besonders stark digitalisiert und damit auf vernetzte IT-Infrastrukturen angewiesen. Dies ist beispielsweise für die Abwicklung hochfrequenter Finanztransaktionen, den Betrieb von Logistikketten oder die Verwaltung sensibler personenbezogener Daten der Fall. Die Unternehmen haben oft viele Schnittstellen zu Kundinnen und Kunden, Patientinnen und Patienten oder Partnerunternehmen, was eine große externe Angriffsfläche mit sich bringt. Aus Sicht von Angreifern sind diese Branchengruppen besonders attraktiv, da erfolgreiche Angriffe dort mit einem hohen Schadenspotenzial verbunden sind. Insbesondere im Gesundheits-

und Sozialwesen sowie im Bildungsbereich existieren oft heterogene, veraltete IT-Strukturen, die das Angriffsrisiko erhöhen können. Demgegenüber weisen etwa Handel sowie Land- und Rohstoffwirtschaft ein niedrigeres Risiko auf.

Tabelle 4-1: Cyberrisiko nach Branchengruppen

Inhärentes Cyberrisiko nach Branchengruppen	Einstufung
SEHR HOHES RISIKO	**5**
HOHES RISIKO	**4**
Gesundheit, Bildung & Soziales	3,9
Finanz- & Versicherungswesen	3,8
Verkehr & Logistik	3,7
MITTLERES RISIKO	**3**
Unternehmensnahe Dienste & Immobilien	2,6
Informations- & Kommunikationswirtschaft	2,4
Sonstige personenbezogene Dienstleistungen	2,4
Industrie	2,4
Energie, Wasser, Entsorgung & Bau	2,3
Handel	2,2
Land- & Rohstoffwirtschaft	2,1
GERINGES RISIKO	**2**
SEHR GERINGES RISIKO	**1**

Durchschnitt von Juni 2024 bis Juli 2025; Einstufung: 5 sehr hohes Risiko, 4 hohes Risiko, 3 mittleres Risiko, 2 geringes Risiko, 1 sehr geringes Risiko; Unternehmen mit 50 bis 250 Beschäftigten

Quelle: Eigene Berechnungen auf Basis von Daten der BitSight Technologies, Inc., bereitgestellt durch Moody's Analytics, Stand: Juli 2025 (n = 17.578). Veröffentlichung mit Genehmigung von BitSight.

Regional betrachtet zeigt sich ein eher homogenes Bild: Alle Bundesländer erreichen Werte zwischen 2,5 und 2,8 – mit Tendenz zum mittleren Risikoniveau. Dabei ist stets zu beachten, dass die Skala relativ ist: Auch Unternehmen mit geringem Risiko können Ziel von Angriffen werden – nur eben statistisch seltener als andere.

Besonders aufschlussreich ist der zeitliche Verlauf des inhärenten Cyberrisikos. Tabelle 4-2 und Abbildung 4-3 dokumentieren, dass das Risiko in einigen Branchen und insgesamt deutlich angestiegen ist, vor allem im ersten Quartal 2025. Gesundheit, Bildung und Soziales erreichen im März und April 2025 fast die höchste Risikostufe. Auch Finanz- und Logistikunternehmen zeigen über mehrere Monate hinweg ein hohes strukturelles Risiko. Eine Studie des IT-Unternehmens Cloudflare, das auf Cybersicherheitslösungen spezialisiert ist, belegt, dass Deutschland im ersten Quartal 2025 weltweit am stärksten von Distributed-Denial-of-Service-Angriffen betroffen war (Cloudflare, 2025). Diese Entwicklung zeigt: Systemische Verwundbarkeiten nehmen schneller zu als Schutzmaßnahmen greifen.

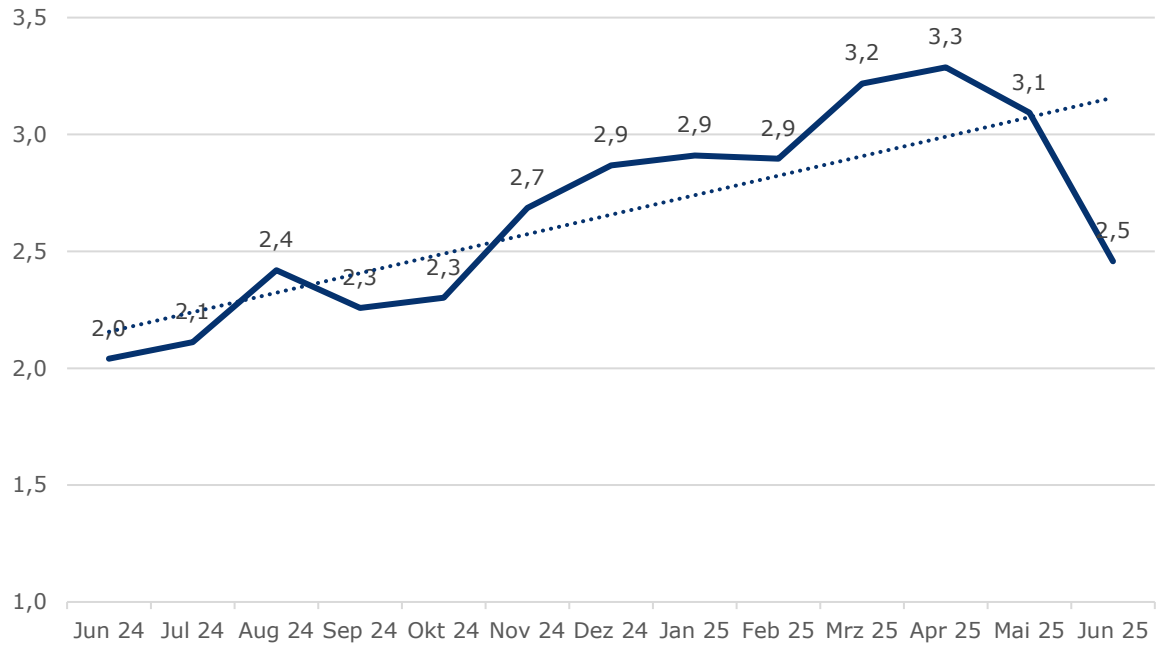
Tabelle 4-2: Cyberrisiko nach Branchengruppen im Zeitverlauf

	Jun 24	Jul 24	Aug 24	Sep 24	Okt 24	Nov 24	Dez 24	Jan 25	Feb 25	Mrz 25	Apr 25	Mai 25	Jun 25
Gesundheit, Bildung & Soziales	2,9	3,1	3,7	3,1	3,1	4	4,1	4,4	4,2	4,9	4,9	4,8	4
Finanz- & Versicherungswesen	3	3,3	3,7	3,1	3,1	3,6	3,9	4	4	4,6	4,6	4,5	3,6
Verkehr & Logistik	3,1	3,2	3,7	3,3	3,3	3,6	3,9	3,9	4	4,2	4,2	4	3,3
Unternehmensnahe Dienste & Immobilien	2	2,1	2,4	2,1	2,1	2,7	2,6	2,7	2,7	3,2	3,3	3,1	2,5
Informations- & Kommunikationswirtschaft	1,9	1,9	2,2	2	2,1	2,3	2,7	2,6	2,7	2,9	3,2	2,7	2,5
Sonstige personenbezogene Dienstleistungen	2	1,9	2,2	2	2	2,5	2,7	2,6	2,8	2,9	2,9	2,7	2,3
Industrie	1,9	1,9	2,1	2,1	2,2	2,4	2,7	2,7	2,7	2,9	2,9	2,8	2
Energie, Wasser, Entsorgung & Bau	1,6	1,6	1,8	2,1	2,2	2,4	2,5	2,6	2,6	3	3	2,7	2
Handel	1,7	1,7	1,9	2	2,1	2,2	2,5	2,5	2,5	2,7	2,7	2,6	2
Land- & Rohstoffwirtschaft	1,4	1,4	1,7	1,7	1,8	2	2,3	2,4	2,3	2,7	2,7	2,6	1,7

Inhärentes Cyberrisiko nach Branchengruppen von Juni 2024 bis Juli 2025 (Monatsdurchschnitte); Einstufung: 5 sehr hohes Risiko, 4 hohes Risiko, 3 mittleres Risiko, 2 geringes Risiko, 1 sehr geringes Risiko

Quelle: Eigene Berechnungen auf Basis von Daten der BitSight Technologies, Inc., bereitgestellt durch Moody's Analytics, Stand: Juli 2025 (n = 17.578). Veröffentlichung mit Genehmigung von BitSight.

Abbildung 4-3: Cyberrisiko im Zeitverlauf



Inhärentes Cyberrisiko von Juni 2024 bis Juli 2025 (Monatsdurchschnitte); Einstufung: 5 sehr hohes Risiko, 4 hohes Risiko, 3 mittleres Risiko, 2 geringes Risiko, 1 sehr geringes Risiko

Quelle: Eigene Berechnungen auf Basis von Daten der BitSight Technologies, Inc., bereitgestellt durch Moody's Analytics, Stand: Juli 2025 (n = 17.578). Veröffentlichung mit Genehmigung von BitSight.

Die vorstehenden empirischen Befunde werden durch Studien untermauert. Laut einer Studie des TÜV (2025) überschätzen viele Unternehmen in Deutschland ihr Cybersicherheitsniveau: 91 Prozent der befragten Unternehmen halten sich für „gut geschützt" – trotz steigender Angriffszahlen und unzureichender technischer Abwehr. In einer Umfrage des Bitkom (2025) gibt die Hälfte der

Unternehmen an, auf Cyberangriffe sehr gut vorbereitet zu sein. Gleichzeitig sehen sich fast drei Viertel der befragten Unternehmen durch Cyberangriffe stark bedroht, 59 Prozent sprechen sogar von einer existenziellen Bedrohung. Knapp drei Viertel der Unternehmen geben an, dass die Anzahl der Cyberattacken auf ihr Unternehmen in den vergangenen 12 Monaten zugenommen hat. Ebenso viele Unternehmen vermuten, dass ihre Informations- und Produktionssysteme oder Betriebsabläufe in den vergangenen 12 Monaten digital sabotiert worden sind. Zwei Drittel der Unternehmen vermuten einen digitalen Diebstahl von Geschäftsdaten in diesem Zeitraum. 82 Prozent gehen davon aus, dass die Anzahl der Cyberattacken weiter steigen wird (ebd.). Technologisch begünstigt wird diese Dynamik durch die wachsende Zahl vernetzter Geräte und täglich neu entdeckter Softwareschwachstellen (78 pro Tag laut BSI, 2024). Diese systemische Verwundbarkeit digitaler Produkte war ein zentrales Motiv für den Cyber Resilience Act, der erstmals verbindliche Cybersicherheitsanforderungen über den gesamten Produktlebenszyklus hinweg definiert (Chiara, 2025).

Insgesamt zeigt die Analyse: KMU bewegen sich auf einem mittleren Sicherheitsniveau – die Cybersicherheitslage ist ausbaufähig. Das strukturelle Risiko nimmt zu, ohne dass dies bislang durch erkennbar verbesserte Schutzmaßnahmen kompensiert wird. Daraus ergibt sich ein klarer Handlungsbedarf. Sowohl technologische als auch regulatorische Entwicklungen verlangen verstärkte und effektive Investitionen in Cybersicherheit. Da die nationale Umsetzung der NIS-2-Richtlinie noch aussteht (Stand: September 2025), fehlt Unternehmen derzeit ein verbindlicher Rechtsrahmen, was die Ausrichtung ihrer Cybersicherheitsmaßnahmen erschwert.

4.2 NIS-2-Richtlinie

4.2.1 Betroffenheitsanalyse

Die NIS-2-Richtlinie betrifft viele Unternehmen direkt. Erfasst werden Organisationen aus 18 Sektoren wie Energie, Verkehr, Gesundheit, digitale Infrastruktur, Finanzwesen, sowie Maschinenbau, Chemie und Lebensmittelindustrie, sofern sie mindestens 50 Beschäftigte oder einen Jahresumsatz und eine Jahresbilanzsumme von mindestens 10 Millionen Euro aufweisen. Unabhängig von Größe und Finanzkennzahlen sind außerdem bestimmte besonders kritische Einrichtungen reguliert, darunter Betreiber kritischer Anlagen nach BSI-Kritisverordnung (Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz) und Anbieter von Vertrauensdiensten. Eine anschauliche Erläuterung der Betroffenheit bietet der Entscheidungsbaum des BSI (2025a). Unter https://betroffenheitspruefung-nis-2.bsi.de/ können Unternehmen ihre Betroffenheit prüfen.

Künftig gelten schätzungsweise 8.250 Unternehmen als besonders wichtige Einrichtungen und rund 21.600 Unternehmen als wichtige Einrichtungen, die dem wirtschaftlichen Sektor zuzuordnen sind (BMI, 2025). Insgesamt sind also rund 29.850 Unternehmen betroffen. Innerhalb der Gruppe der besonders wichtigen Einrichtungen sind 4.693 Unternehmen bereits heute als Anbieter digitaler Dienste oder Betreiber kritischer Anlagen nach geltender Rechtslage zur Umsetzung entsprechender Sicherheitsmaßnahmen verpflichtet. Für die verbleibenden rund 25.200 Unternehmen begründet NIS-2 neue Verpflichtungen – unter anderem zur Einführung eines Risikomanagements, zur technischen Absicherung und zur Meldung schwerwiegender Sicherheitsvorfälle (ebd.).

Auch mittelbar wirkt die NIS-2-Richtlinie auf zahlreiche Unternehmen: Direkt regulierte Einrichtungen müssen ihre Lieferkette absichern, etwa durch vertragliche Anforderungen an die betriebliche Cybersicherheit. Betroffen sind hier unter anderem Anbieter von IT-Hardware und -Software, Managed (Security) Service Provider und Cloud-Dienstleister (BMI, 2025; ENISA, 2025). Die genaue Zahl indirekt betroffener Unternehmen lässt sich schwierig beziffern, da sie je nach Branche, Geschäftsmodell und Unternehmensgröße stark variiert. Eine rein illustrative Annahme von durchschnittlich sieben kritischen Dienstleistern oder Zulieferern pro reguliertem Unternehmen – unter Berücksichtigung von Überschneidungen – deutet bereits auf mehr als 200.000 mittelbar betroffene Unternehmen hin.

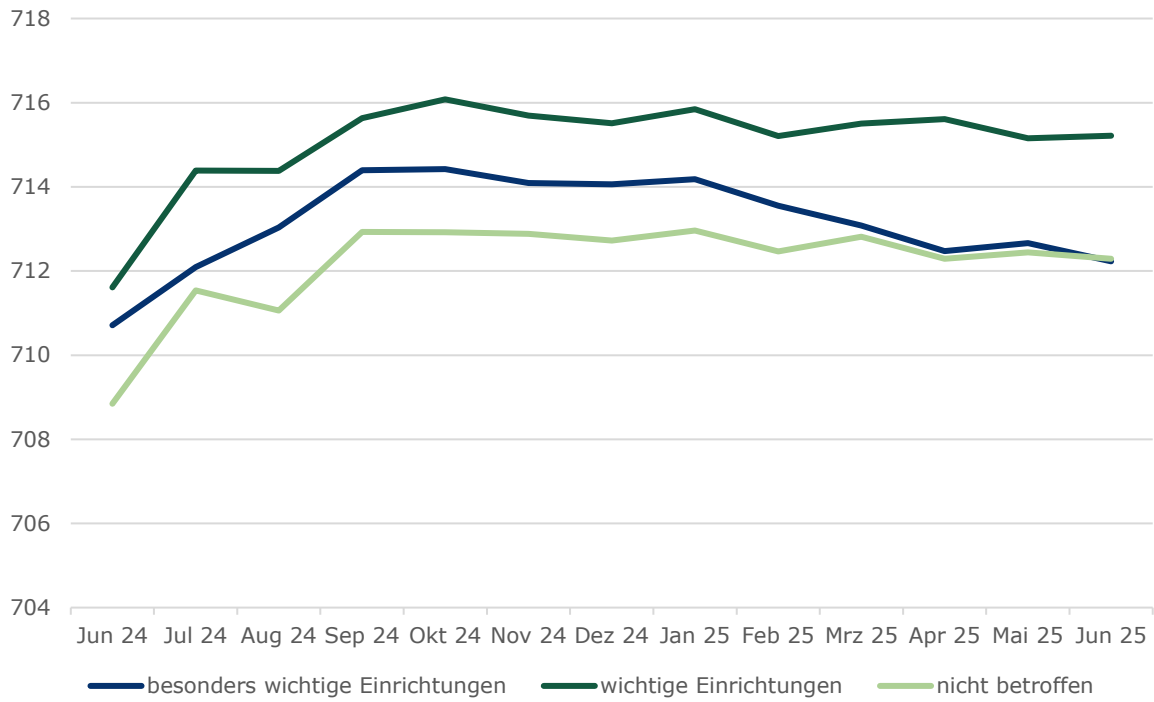
In der Summe führt die NIS-2-Richtlinie damit zu einem massiven Zuwachs an Unternehmen, die erstmals regulatorischen Pflichten im Bereich Cybersicherheit unterliegen – mit entsprechender Nachfrage nach Informations-, Beratungs- und Schulungsangeboten in einem nie dagewesenen Ausmaß.

4.2.2 Ausgangslage der betroffenen Unternehmen

Um die Auswirkungen der NIS-2-Richtlinie auf Unternehmen in Deutschland einschätzen zu können, wurde im Rahmen dieser Studie analysiert, wie hoch das extern beobachtbare Cybersicherheitsniveau jener Unternehmen ist, die voraussichtlich unter die Regulierung fallen. Grundlage der Analyse ist die Stichprobe der Orbis Datenbank mit 17.578 Unternehmen mit 50 bis 250 Beschäftigten. Zunächst wurden diese Unternehmen den beiden Adressatengruppen der NIS-2-Richtlinie zugeordnet: besonders wichtige Einrichtungen und wichtige Einrichtungen. Die Einordnung erfolgte anhand des NACE Rev. 2-Codes (Haupttätigkeit) und einer Schwellenwertprüfung nach Beschäftigtenzahl, Umsatz und Bilanzsumme. Einrichtungen, deren Relevanz nicht über NACE-Codes bestimmbar ist – wie etwa Betreiber kritischer Anlagen gemäß BSI-Kritisverordnung, Telekommunikationsdiensteanbieter oder Vertrauensdiensteanbieter – konnten mangels identifizierbarer Merkmale in Orbis nicht berücksichtigt werden.

Insgesamt wurden 1.008 mittelständische Unternehmen (5,7 Prozent) als besonders wichtige Einrichtungen und 4.610 mittelständische Unternehmen (26,2 Prozent) als wichtige Einrichtungen eingeordnet. Die übrigen 11.960 Unternehmen (68,0 Prozent) aus der Stichprobe sind nach dieser Logik nicht direkt von der NIS-2-Richtlinie betroffen. Zu beachten ist, dass es sich um eine nichtrepräsentative Stichprobe handelt. Die Befunde sind daher als indikativ zu interpretieren und lassen keine direkte Hochrechnung auf alle betroffenen Unternehmen zu.

Abbildung 4-4: Cybersicherheitsrating nach NIS-2-Einstufung im Zeitverlauf



Durchschnittliches Cybersicherheitsniveau nach NIS-2-Einstufungskategorie von Juni 2024 bis Juli 2025 (Monatsdurchschnitt); Ratingeinstufung: grundlegend (250–639), mittel (640–739), fortgeschritten (740–900); betrachtete Unternehmen: 50 bis 250 Beschäftigte

Quelle: Eigene Berechnungen auf Basis von Daten der BitSight Technologies, Inc., bereitgestellt durch Moody's Analytics, Stand: Juli 2025 (n = 17.578). Veröffentlichung mit Genehmigung von BitSight.

Das durchschnittliche Cybersicherheitsrating unterscheidet sich nur geringfügig zwischen den verschiedenen NIS-2-Kategorien: Besonders wichtige Einrichtungen erreichen im Analysezeitraum Juni 2024 bis Juni 2025 einen Durchschnittswert von 713 Punkten, wichtige Einrichtungen liegen bei 715 Punkten und nicht betroffene Einrichtungen bei 712 Punkten. Über den gesamten Zeitraum zeigt sich ein leichter Anstieg des Sicherheitsniveaus (Abbildung 4-4). Das Fehlen substanzieller Unterschiede zwischen den Gruppen legt nahe, dass viele betroffene Unternehmen bislang noch nicht mit der Umsetzung der NIS-2-Anforderungen begonnen haben oder dass die Umsetzung (noch) nicht zu sichtbaren Verbesserungen in extern messbaren Sicherheitskennzahlen geführt hat.
Eine genauere Betrachtung der vier Risikodimensionen des Ratings, die mittels Schulnoten von 1 (sehr gut) bis 6 (ungenügend) bewertet wurden, zeigt ein differenzierteres Bild. Die zugrunde liegenden Werte basieren auf einem Durchschnitt aus den Monaten April bis Juni 2025 und erlauben somit eine aktuelle Einschätzung des technischen Sicherheitsprofils.

Obwohl das Cybersicherheitsrating der Unternehmen insgesamt nur im mittleren Bereich liegt, werden in den einzelnen Risikodimensionen gute bis sehr gute Noten erreicht. Das ist methodisch plausibel: Die einzelnen Risikovektoren werden relativ – als Perzentile – gegenüber der Gesamtpopulation der bewerteten Organisationen eingeordnet, bevor aus den gewichteten Vektorwerten ein Gesamtscore gebildet wird, der regelmäßig normalisiert wird. So können viele Unternehmen in einzelnen Vektoren gut erscheinen, während die gewichtete Summe und die Normalisierung die Gesamtratings breiter über die Skala verteilen. Hinzu kommt eine explizite Zeitkomponente: Kompromittierungen und Cybersicherheitsvorfälle haben eine Nachwirkung, weil sie künftiges Risiko anzeigen. Daher können aktuelle Dimensionen gut bewertet sein, während das Gesamtrating durch Vorfälle weiterhin gedämpft bleibt. Schließlich trägt die sehr ungleiche Gewichtung der Dimensionen dazu bei, dass sich gute Teilnoten und ein nur mittleres Gesamtergebnis nicht widersprechen.

Ausgerechnet in der zentralen Dimension „Sicherheitsstandards", die mit 70,5 Prozent in das Gesamtrating einfließt, schneiden die Unternehmen am schwächsten ab (Tabelle 4-3). Besonders wichtige Einrichtungen erreichen hier mit einem Durchschnitt[7] von 2,01 nur leicht bessere Werte als nicht betroffene Unternehmen (2,03). Angesichts der erhöhten Schutzpflichten ist das Ergebnis sicherheitsstrategisch bedenklich: Die Unternehmen, die den strengsten Pflichten nachkommen werden müssen, weisen bei der technisch unmittelbar gestaltbaren grundsätzlichen Cyberhygiene kein signifikant besseres Sicherheitsniveau auf als die von NIS-2 nicht betroffenen Unternehmen.

In der Dimension „Kompromittierte Systeme" (Gewichtung: 27 Prozent) erzielen alle Gruppen sehr gute Werte zwischen 1,03 und 1,07. Zu berücksichtigen ist hierbei, dass kompromittierende Ereignisse gemäß der Rating-Methodik die einzelnen Vektoren der Dimension nahe am Ereignistag stark beeinflussen, aber mit der Zeit abklingen. Dadurch können aktuelle Noten sehr gut sein, obwohl einzelne Vorfälle (auch vor den Monaten April bis Juni 2025) das Gesamtrating weiterhin dämpfen können.

Das „Nutzendenverhalten" fließt mit 2,5 Prozent ins Rating ein und misst riskante Interaktionen wie unsichere Datenfreigaben. Besonders wichtige Einrichtungen schneiden hier mit 1,24 schlechter ab als wichtige Einrichtungen (1,14) oder nicht betroffene Unternehmen (1,19), was auf kulturelle oder prozessuale Schwächen in sicherheitsrelevanten Alltagspraktiken hindeuten könnte.

Am besten schneiden die Unternehmen in der Risikodimension „Sicherheitsvorfälle" ab, über die öffentlich gewordene Datenlecks oder Ransomwareangriffe je nach Schwere in das Cybersicherheitsrating einfließen. Der Mittelwert liegt hier konstant bei 1,02 über alle Unternehmensgruppen

[7] Obwohl es sich bei Schulnoten formal um ordinalskalierte Daten handelt, werden diese in der vorliegenden Analyse als quasi-intervallskaliert behandelt, um arithmetische Mittelwerte berechnen und Gruppenvergleiche durchführen zu können; diese Vorgehensweise entspricht gängiger Praxis in Bildungsforschung und amtlicher Statistik.

hinweg. Methodisch relevant ist, dass schwere Vorfälle als zusätzlicher Korrekturschritt im Gesamtrating berücksichtigt werden. Diese Korrekturkomponente ist abhängig von Unternehmensgröße und Vorfallsschwere und klingt mit der Zeit ab. Dadurch kann die betreffende Risikodimension aktuell sehr gut bewertet sein, während das Gesamtrating wegen der fortwirkenden Effekte früherer schwerer Vorfälle niedriger bleibt.

Tabelle 4-3: Risikodimensionen des Cybersicherheitsratings

	besonders wichtige Einrichtungen	wichtige Einrichtungen	nicht betroffene Einrichtungen
Sicherheitsstandards	2,01	2,00	2,03
Kompromittierte Systeme	1,07	1,03	1,06
Nutzendenverhalten	1,24	1,14	1,19
Sicherheitsvorfälle	1,02	1,02	1,02

Abschneiden der Unternehmen je nach NIS-2-Kategorie in den vier Risikodimensionen des Cybersicherheitsratings; Note 1 (fortgeschritten, sehr gut; grün) bis 6 (ungenügend; rot); Unternehmen mit 50 bis 250 Beschäftigten
Quelle: Eigene Berechnungen auf Basis von Daten der BitSight Technologies, Inc., bereitgestellt durch Moody's Analytics, Stand: Juli 2025 (n = 17.578). Veröffentlichung mit Genehmigung von BitSight.

Besonders auffällig ist bei der Analyse der einzelnen Risikodimensionen, dass besonders wichtige Einrichtungen – trotz der unter NIS-2 geltenden strengsten Pflichten – keine durchgängig besseren Sicherheitswerte aufweisen. Das deutet darauf hin, dass viele Unternehmen bislang noch nicht mit der Umsetzung begonnen haben oder vor allem organisatorische, aber keine technischen Fortschritte erzielt wurden. Tatsächlich kennt nur gut die Hälfte der vom TÜV (2025) befragten Unternehmen die NIS-2-Richtlinie.

4.2.3 Zentrale Herausforderungen im Kontext der NIS-2-Richtlinie

Die vorstehenden Analysen zeigen, dass KMU in Deutschland insgesamt zu wenig cybersicher sind, gemessen an dem Niveau, das eine funktionsfähige und resiliente Volkswirtschaft mit kritischen Abhängigkeiten erfordert. Die beobachteten guten Teilnoten sind nicht als Entwarnung zu lesen. Zum einen handelt es sich um relative Bewertungen: Die Einordnung per Perzentil und die regelmäßige Normalisierung sorgen für Vergleichbarkeit, markieren aber keinen Zielzustand. Ein „gut" signalisiert relative Stärke, nicht das Erreichen eines ambitionierten Soll-Niveaus. Zum anderen sind die Gewichte der Risikodimensionen stark ungleich verteilt. In der hoch gewichteten Dimension „Sicherheitsstandards" werden im Durchschnitt nur Zweier-Noten erreicht, einzelne Risikovektoren verbleiben sogar nur im befriedigenden Bereich. Das dokumentiert, dass Mindeststandards nicht flächendeckend durchgesetzt sind. Cybersicherheit erfordert jedoch, umfassend geschützt zu sein und bei allen Risikovektoren sehr gut abzuschneiden. Cyberkriminellen genügt oft ein kleines Einfallstor, um großen Schaden anzurichten. Schließlich wirkt die Zeitkomponente gegen trügerische Momentaufnahmen: Vorfälle und kompromittierte Systeme beeinflussen das Gesamtrating über die Zeit, sodass gute aktuelle Teilwerte ein strukturell zu niedriges Gesamtniveau nicht kompensieren.

Zudem bildet das externe Cybersicherheitsrating interne Governance-Elemente nicht ab, die für NIS-2 konstitutiv sind. Wenn Unternehmen bei extern beobachtbaren Cybersicherheitsmaßnahmen nur Durchschnitt erreichen und zugleich zentrale organisatorische Fähigkeiten – Risikomanagement, Incident Response und Business Continuity – nicht belastbar nachweisen, steigen Ausfallrisiken, die Allokation knapper IT-Sicherheitsressourcen verschlechtert sich und negative Externalitäten entlang von Lieferketten nehmen zu (vgl. Arroyabe et al., 2024). Regulierungspolitisch drohen damit einerseits Nicht-Konformität und damit verbundene Kosten, andererseits bleibt das

operative Restrisiko hoch, weil wirksame Sicherheitsmaßnahmen nicht auf ein hohes Niveau gebracht werden. Die gemessenen Defizite in den Sicherheitsstandards verweisen auf technische Schwächen, die NIS-2-relevante Anforderungen betreffen. Gerade vor dem Inkrafttreten der neuen Vorgaben zeigt sich hier ein erheblicher Handlungsbedarf, insbesondere im Bereich technischer Konfiguration und Sorgfalt. Maßnahmen wie das Schließen offener Ports, die Erneuerung veralteter Zertifikate und Protokolle oder die Einführung sicherer E-Mail-Authentifizierung sind technisch direkt adressierbar und eignen sich als erste Ansatzpunkte für sichtbare Verbesserungen.
Die insgesamt durchschnittliche Ausgangslage vieler Unternehmen im Bereich der extern beobachtbaren Cybersicherheit darf nicht darüber hinwegtäuschen, dass substanzielle Herausforderungen bestehen. Cybersicherheit erfordert nicht nur technische Schutzmaßnahmen, sondern auch kontinuierliche Wartung, Anpassung und organisatorische Verankerung – wofür personelle und finanzielle Ressourcen nötig sind.

Eine zentrale Herausforderung ist der Fachkräftemangel. Viele Unternehmen verfügen nicht über ausreichend IT-Fachkräfte. Gerade kleinere Unternehmen sind im Wettbewerb um Talente gegenüber Großunternehmen strukturell im Nachteil. Das kann dazu führen, dass Sicherheitsmaßnahmen verzögert, lückenhaft oder gar nicht umgesetzt werden. Laut einer globalen Erhebung von Fortinet (2024) berichteten 90 Prozent der befragten Unternehmen im Jahr 2023 von mindestens einem Sicherheitsvorfall, der teilweise auf fehlende Cybersicherheitskompetenzen zurückzuführen war. 70 Prozent machten den Mangel an Fachpersonal explizit für erhöhte Risiken verantwortlich, fast 60 Prozent sahen unzureichende Aus- und Weiterbildung der Mitarbeitenden als zentrale Ursache für Cybersicherheitsvorfälle. Cybersicherheitskompetenzen sind stark nachgefragt: Die Anzahl der Online-Stellenanzeigen mit entsprechenden Anforderungsprofilen hat sich zwischen 2019 und 2024 von rund 117.000 auf über 203.000 nahezu verdoppelt (Büchel/Engels, 2025). Der strukturelle Fachkräftemangel dürfte sich weiter verschärfen. Der Bitkom (2024c) prognostiziert bis 2040 eine Lücke von rund 663.000 IT-Fachkräften. Besonders betroffen sind laut dem Global Cybersecurity Outlook des World Economic Forum Sektoren wie Bildung und Gesundheit, die öffentliche Verwaltung sowie KMU (WEF, 2025).

Neben dem Fachkräftemangel stellt auch die geringe organisatorische und technologische Reife vieler KMU eine zentrale Herausforderung dar. Unternehmen, die bislang nicht durch Regulierungen wie die BSI-Kritisverordnung erfasst waren und daher auch noch keine gesetzlich verbindlichen Cybersicherheitsanforderungen erfüllen mussten, verfügen häufig weder über ein systematisches Sicherheitsmanagement noch über klar geregelte Zuständigkeiten. Technische Defizite treffen so auf eine fehlende Sicherheitskultur. Hinzu kommt, dass Cybersicherheit in kleinen Unternehmen vielfach – auch wegen starker Budgetrestriktionen – vor allem als Kostenfaktor betrachtet wird und weniger als strategischer Werttreiber.

Die Umsetzung der NIS-2-Anforderungen wird dadurch insbesondere für KMU zur strukturellen, personellen und finanziellen Belastung.

4.2.4 Kosten im Kontext der NIS-2-Richtlinie

Die Einhaltung der NIS-2-Anforderungen ist für Unternehmen mit Investitionen in technische, organisatorische und personelle Sicherheitsmaßnahmen verbunden. Der Referentenentwurf zur Umsetzung der Richtlinie (BMI, 2025) liefert eine detaillierte Abschätzung der finanziellen Auswirkungen auf die Wirtschaft. Er unterscheidet zwischen einmaligen und laufenden Kosten (einmaliger vs. jährlicher Erfüllungsaufwand).

Für besonders wichtige Einrichtungen wird ein jährlicher Erfüllungsaufwand allein für die Einhaltung eines Mindestniveaus an IT-Sicherheit von rund 215.000 Euro pro Unternehmen angenommen. Dieser setzt sich zusammen aus Personalkosten für etwa 2.752 Stunden zu einem Lohnsatz von 56,08 Euro sowie Sachkosten in Höhe von 60.700 Euro. Bei wichtigen Einrichtungen wird von einem geringeren Aufwand ausgegangen: Hier werden 1.100 Stunden Personalkosten sowie

24.300 Euro Sachkosten kalkuliert – insgesamt etwa 86.000 Euro jährlich. Zusätzlich entstehen jährliche Kosten durch Informationspflichten und regelmäßige Schulungen der Geschäftsleitung.

Der einmalige Erfüllungsaufwand wird in beiden Kategorien jeweils in etwa so hoch eingeschätzt wie der jährliche Aufwand. Er entfällt vor allem auf die Einführung oder Anpassung digitaler Prozesse, etwa den Aufbau eines Informationssicherheits-Managementsystems, die Umsetzung sicherer Authentifizierungsverfahren sowie die Etablierung von Meldeprozessen für Sicherheitsvorfälle.

Die gesamtwirtschaftliche Belastung wird auf Grundlage von 2.950 besonders wichtigen und 17.900 wichtigen Einrichtungen berechnet, die bislang keine vergleichbaren Pflichten erfüllen und kein hohes IT-Sicherheitsniveau aufweisen. Daraus ergibt sich ein einmaliger Aufwand von rund 2,2 Milliarden Euro sowie ein jährlicher Aufwand von etwa 2,3 Milliarden Euro. Der zusätzliche bürokratische Aufwand durch neue Dokumentations-, Nachweis- und Meldepflichten wird mit 2,8 Millionen Euro jährlich vergleichsweise gering eingeschätzt.

Dennoch stellt die Umsetzung für viele Unternehmen – insbesondere KMU – eine spürbare Belastung dar, vor allem wenn bisher keine entsprechenden Strukturen existieren. KMU stehen vor der Herausforderung, fehlende fachliche Expertise und mangelnde Umsetzungserfahrung zu kompensieren (BMI, 2025). Unternehmen, die bereits relevante Normen und Standards im Bereich Cybersicherheit umsetzen, dürften mit einem geringeren Zusatzaufwand konfrontiert sein. Immerhin 22 Prozent der vom TÜV (2025) befragten Unternehmen ab zehn Beschäftigten geben an, bestimmte Normen und Standards für die IT-Sicherheit vollständig zu erfüllen. Weitere 53 Prozent setzen sie zumindest teilweise um.

KMU mit begrenzten finanziellen Spielräumen könnten sich mit der Herausforderung konfrontiert sehen, notwendige Investitionen in Digitalisierung, Innovation oder Weiterbildung zugunsten regulatorischer Compliance aufschieben zu müssen. Das könnte sich negativ auf die Wettbewerbsfähigkeit und Innovationskraft der betroffenen Unternehmen auswirken.

Darüber hinaus zeigen sich indirekte Belastungseffekte, die über die direkt adressierten Unternehmen hinausreichen: Auch Unternehmen, die formal nicht direkt der NIS-2-Richtlinie unterliegen, sehen sich als Zulieferer oder Dienstleister für direkt regulierte Unternehmen verstärkt vertraglichen Anforderungen und Prüfpflichten gegenüber, die faktisch eine NIS-2-konforme Sicherheitsstruktur voraussetzen.

4.2.5 Nutzen der NIS-2-Richtlinie

Die Kosten für die Umsetzung der NIS-2-Richtlinie sind gerade für kleinere Unternehmen mit begrenzten Ressourcen deutlich spürbar. Im Verhältnis zum potenziellen Nutzen erscheinen diese jedoch vertretbar, zumal sich bereits durch eine moderate Reduktion von Cyberschäden ein volkswirtschaftlicher Mehrwert erzielen lässt.

Allein im vergangenen Jahr ist deutschen Unternehmen durch Cyberangriffe ein Schaden von 202,4 Milliarden Euro entstanden (Bitkom, 2025a). Demgegenüber belaufen sich die geschätzten jährlichen Umsetzungskosten der NIS-2-Richtlinie auf lediglich rund 1,1 Prozent dieser Schadenssumme. Bereits eine Reduktion der Cyberschäden durch die höheren Cybersicherheitsniveaus gemäß NIS-2 um 1,1 Prozent würde die Regulierung aus volkswirtschaftlicher Perspektive rechtfertigen.

Neben der Vermeidung direkter wirtschaftlicher Schäden bringt die Umsetzung der NIS-2-Richtlinie für viele Unternehmen weitere Vorteile mit sich. Insbesondere für KMU, die bislang keine vergleichbaren regulatorischen Pflichten kannten, kann die Einführung eines strukturierten Informationssicherheitsmanagements einen wichtigen Impuls zur organisatorischen Professionalisierung darstellen. Die klare Zuweisung von Verantwortlichkeiten, die verpflichtende Risikobewertung sowie regelmäßige Schulungen tragen dazu bei, Cybersicherheit systematisch im Unternehmen zu verankern. Dies stärkt nicht nur die Resilienz gegenüber externen Angriffen, sondern verbessert auch die Handlungsfähigkeit im Krisenfall. Unternehmen sind in der Lage, im Ernstfall schneller,

koordinierter und effektiver zu reagieren, wodurch Produktionsunterbrechungen verkürzt und Reputationsverluste minimiert werden.

Auch strukturell entstehen Impulse zur Effizienzsteigerung. Die Umsetzung der NIS-2-Vorgaben erfordert häufig eine grundlegende Bestandsaufnahme bestehender IT-Prozesse. Veraltete oder ineffiziente Strukturen werden identifiziert und durch sichere, modernere Systeme ersetzt – ein Schritt, der langfristig auch die betriebliche Leistungsfähigkeit verbessert.

Nicht zuletzt kann ein nachweislich hohes Cybersicherheitsniveau zu einem Wettbewerbsvorteil werden. In sensiblen Wertschöpfungsketten gewinnen Unternehmen mit zertifizierter Sicherheit an Attraktivität, qualifizieren sich leichter für öffentliche Ausschreibungen und stärken ihre Position bei Geschäftspartnern. Auch für Fachkräfte gewinnt die Frage der IT-Sicherheit an Bedeutung, sodass ein professionelles Sicherheitsmanagement zur Arbeitgeberattraktivität beiträgt.

Trotz der initialen Investitionen und des laufenden Aufwands kann die Umsetzung der NIS-2-Richtlinie somit mittelfristig betriebswirtschaftliche und strategische Mehrwerte generieren. Insgesamt ist zu erwarten, dass das Cybersicherheitsniveau in Deutschland steigt.

4.3 Cyber Resilience Act

4.3.1 Betroffenheitsanalyse

Es ist aus mehreren Gründen schwierig einzuschätzen, wie viele Unternehmen vom Cyber Resilience Act betroffen sind. Anders als die NIS-2-Richtlinie beschränkt sich der CRA nicht auf bestimmte Branchen oder Unternehmensgrößen. Vielmehr ist er produktbezogen und verpflichtet unterschiedliche Wirtschaftakteure, die digitale Produkte in Verkehr bringen oder bereitstellen– darunter Hersteller, Einführer, Händler, Bevollmächtigter oder unter bestimmten Bedingungen auch Verwalter quelloffener Software (vgl. Arzt et al., 2025). Der CRA gilt dabei nur für Produkte mit digitalen Elementen oder Software, die ab Ende 2027 erstmals neu auf den Markt gebracht werden.

- Als Hersteller gilt nicht nur, wer ein Produkt entwickelt oder produziert, sondern auch, wer es unter eigenem Namen vertreibt – selbst wenn es von Dritten hergestellt wurde. Händler oder Einführer können ebenfalls als Hersteller eingestuft werden, wenn sie Produkte wesentlich verändern oder unter eigener Marke vertreiben.
- Einführer sind Unternehmen mit Sitz in der EU, die Produkte aus Drittstaaten in den europäischen Binnenmarkt bringen,
- während Händler diese Produkte lediglich bereitstellen, ohne Hersteller oder Einführer zu sein.
- Hersteller außerhalb der EU, deren Produkte in der EU vertrieben werden, müssen einen in der EU ansässigen Bevollmächtigten benennen, der Verpflichtungen wie die Aufbewahrung der EU-Konformitätserklärung sowie die Bereitstellung technischer Unterlagen für Marktaufsichtsbehörden übernimmt.
- Verwalter quelloffener Software unterliegen dem CRA, wenn sie Projekte betreiben, die in kommerziellen Produkten verwendet werden und organisatorisch strukturiert sind sowie dauerhaft in einem geschäftlichen Umfeld betrieben werden.

Welche Rolle ein Unternehmen in Bezug auf ein konkretes Produkt einnimmt, hängt demnach vom individuellen Herstellungsprozess und Vertriebsmodell ab und lässt sich nicht aus öffentlich verfügbaren Unternehmensdaten ableiten.

Da Produkte mit digitalen Elementen branchenübergreifend verbreitet sind, ist der Anwendungsbereich des CRA nicht auf bestimmte Wirtschaftszweige begrenzt. Vom Stück- und Umsatzvolumen her dürfte die Industrie der Unterhaltungselektronik am stärksten betroffen sein. Zum Markt der verbrauchernahen vernetzbaren Produkte, die ebenfalls unter den CRA fallen, gehören darüber hinaus auch vernetzbare Haushaltsgeräte. Ebenfalls betroffen sind die Hersteller weiterer elektronischer und elektrischer Ausrüstungen, der Maschinen- und Anlagenbau sowie Sensorik und Automatisierungstechnik, soweit Produkte mit integrierter Software hergestellt werden. Die

Informations- und Kommunikationswirtschaft ist vor allem aufgrund der Vielzahl an Anbietern, darunter Softwareentwickler und IT-Dienstleister, besonders betroffen. Hinzu kommt der Handel mit IKT-Geräten, vernetzten Haushaltsgeräten, Unterhaltungselektronik oder Wearables. Weniger betroffen sind typischerweise Dienstleistungsbranchen wie das Finanz-, Gesundheits- oder Bildungswesen, die digitale Produkte vorwiegend nutzen, aber nur selten selbst vertreiben oder herstellen. Für sie können jedoch mittelbare Anforderungen entstehen, etwa bei der Integration externer Softwarekomponenten.

Eine belastbare Quantifizierung des vom CRA betroffenen Unternehmenskreises ist aufgrund der komplexen, rollen- und produktbezogenen Ausgestaltung der Verordnung kaum möglich. Dennoch wird im Folgenden ein Näherungswert ermittelt (siehe Tabelle 4-4). Für die Schätzung der direkt betroffenen Unternehmen wird – ähnlich wie im Impact Assessment der Europäischen Kommission (European Commission, 2022) – zwischen einer konservativen und einer erweiterten Variante unterschieden. Die Schätzungen beruhen jedoch auf eigenständigen Berechnungen und erweitern die Methodik des Impact Assessments um zusätzliche Branchen und Annahmen.[8]

- Konservative Variante: Beschränkung auf Kernbranchen der IKT-Produktion (Software und Hardware); bereinigt um Kleinstunternehmen im Bereich Programmierung. Bei diesen Kleinstunternehmen wird davon ausgegangen, dass sie vor allem Auftragsprogrammierung machen, das heißt, sie entwickeln die Software im Kundenauftrag und der Kunde bringt das Endprodukt unter seinem Namen in Verkehr. Dann ist der Auftraggeber der Hersteller und der Dienstleister ist kein wirtschaftlicher Akteur, der unter den CRA fällt. Zusätzlich werden Handelsunternehmen einbezogen, deren Tätigkeit unmittelbar auf den Vertrieb von Produkten mit digitalen Elementen gerichtet ist, denn sie gelten unter dem CRA als Händler, die vor der Marktbereitstellung prüfen müssen, ob das Produkt die CE-Kennzeichnung trägt und von einer EU-Konformitätserklärung begleitet wird.
- Erweiterte Variante: Ergänzend zu den Kernbranchen werden weitere Fertigungssektoren wie beispielsweise die Herstellung von Datenverarbeitungsgeräten und die Herstellung von elektrischen Ausrüstungen berücksichtigt, die potenziell Produkte mit digitalen Elementen enthalten könnten.[9] Die Programmierungsbranche wird vollständig einbezogen. Die Handelsunternehmen werden in gleicher Anzahl wie in der konservativen Variante einbezogen.

Für die Softwarebranche waren in Deutschland 2023 rund 45.974 Unternehmen registriert (Statistisches Bundesamt, 2025). Da der überwiegende Teil Kleinstunternehmen im Bereich Programmierung (NACE J62.01) sind, die voraussichtlich nicht unter den CRA fallen, wurde diese Branche in der konservativen Schätzung um 88 Prozent auf rund 6.900 Unternehmen reduziert.[10]

Für die Hardwarebranche ergibt sich je nach Abgrenzung ein Umfang von rund 4.400 (konservativ) bis 46.900 (erweitert) Unternehmen.

Die einbezogenen Handelsunternehmen entsprechen den NACE-Codes 47.4 (Einzelhandel mit IKT-Geräten), 46.5 (Großhandel mit IKT-Geräten), 46.43 (Großhandel mit Haushalts-, Foto- und Unterhaltungselektronik) sowie 47.54 (Einzelhandel mit elektrischen Haushaltsgeräten). Zusammengenommen ergibt dies 27.021 Unternehmen. Diese Zahl gilt für beide Varianten, da

[8] Verwendete NACE Rev2.-Codes: Software: J58.2, J62.01; Hardware (konservativ): C26.1, C26.2, C26.3, C26.4, C26.8; Hardware (erweitert): C26, C27, C28, C30, C32. Die NACE-Klasse C33 (Reparatur und Installation von Maschinen und Ausrüstungen) wurde in der vorliegenden Analyse – anders als im Impact Assessment – nicht berücksichtigt, da diese Unternehmen in der Regel keine eigenen Produkte mit digitalen Elementen in Verkehr bringen und damit nicht unmittelbar unter den Anwendungsbereich des CRA fallen. Ihre Tätigkeit beschränkt sich auf die Wartung und Reparatur bereits im Umlauf befindlicher Produkte. Außerdem wurde C32.1 (Herstellung von Münzen, Schmuck und ähnlichen Erzeugnissen) ausgeschlossen.

[9] Das Impact Assessment (European Commission, 2023) quantifiziert den europäischen Software- und Hardwaremarkt auf Basis der IKT-Produktion und zieht in der erweiterten Variante auch digitale Produkte in nicht-digitalen Fertigungssektoren heran. Dort wird ein sogenannter „digitaler Intensitätsfaktor" eingesetzt, der den Anteil digitaler Prozesse als Proxy für den Anteil digitaler Endprodukte nutzt. Diese Methode wird in dieser Analyse nicht übernommen, da digitale Prozesse nicht zwangsläufig auf digitale Produkte schließen lassen.

[10] Laut einer Sonderauswertung des Statistischen Bundesamts hatten im Jahr 2022 rund 88 Prozent der Unternehmen in der NACE-Klasse 62 (IT-Dienstleistungen) höchstens zehn Mitarbeitende.

keine verlässliche Datengrundlage existiert, um die Zahl im konservativen beziehungsweise erweiterten Szenario unterschiedlich abzugrenzen. Diese Schätzung ist jedoch mit Einschränkungen verbunden: Die konkrete Marktrolle als Einführer oder Händler lässt sich über die NACE-Systematik nicht eindeutig erfassen, da diese sich nicht aus dem Wirtschaftszweig, sondern aus dem konkreten Produktbezug und Vertriebsweg ergibt. Zudem ist nicht erkennbar, ob tatsächlich Produkte mit digitalen Elementen vertrieben werden – dies ist jedoch Voraussetzung für die Anwendbarkeit des CRA. Auch lässt sich nicht abbilden, ob ein Unternehmen ein Produkt substanziell verändert oder unter eigenem Namen vertreibt, was wiederum darüber entscheidet, ob es rechtlich als Hersteller gilt.

In Summe ergibt sich ein Schätzkorridor von etwa 38.000 bis 120.000 potenziell vom CRA betroffenen Unternehmen. Diese Zahlen sind nicht als juristisch belastbare Schätzung zu verstehen, sondern dienen als erste Orientierung für den Umfang der Betroffenheit. Gleichzeitig verdeutlicht die Schätzung die Herausforderung, den Geltungsbereich des CRA statistisch belastbar zu bestimmen.

Tabelle 4-4: Schätzung der Anzahl der Unternehmen (gerundet), die direkt unter den Cyber Resilience Act fallen

Schätzung	Software	Hardware	Handel	Gesamt
konservativ	6.900	4.400	27.000	38.300
erweitert	46.000	46.900	27.000	119.900

Quelle: eigene Berechnungen basierend auf Statistisches Bundesamt (2025).

Der tatsächliche Kreis der betroffenen Akteure dürfte noch größer sein. Zwar kennt der CRA – anders als die NIS-2-Richtlinie – formal keine mittelbar betroffenen Unternehmen. In der Praxis ist jedoch davon auszugehen, dass rechtliche Pflichten entlang der Wertschöpfungsketten weitergegeben werden. Software-Dienstleister, Komponentenhersteller oder OEM-Zulieferer dürften in die Pflichterfüllung eingebunden werden, selbst wenn sie nicht unmittelbar adressiert sind.

4.3.2 Ausgangslage der betroffenen Unternehmen

Der CRA ist produktzentriert und adressiert Sicherheitsanforderungen an Produkte mit digitalen Elementen, nicht die organisationale Cybersicherheit eines Unternehmens im engeren Sinne. Das Cybersicherheitsrating, das zur Einschätzung der Ausgangslage von Unternehmen im Kontext der NIS-2-Richtlinie herangezogen wurde, misst hingegen ausschließlich extern beobachtbare Merkmale wie Angriffsfläche, IT-Konfiguration oder öffentlich sichtbare Schwachstellen in Unternehmensnetzwerken. Es liefert keine Informationen zu produktspezifischen Sicherheitsmerkmalen, wie sie im CRA zentral gefordert werden, etwa zur technischen Dokumentation, zur CE-Kennzeichnung oder zum Schwachstellenmanagement.

Daher ist das Cybersicherheitsrating nur eingeschränkt geeignet, um die Ausgangslage von Unternehmen im CRA-Kontext zu erfassen. Es kann bestenfalls als Proxy für die organisatorisch-technische Reife eines Unternehmens dienen – und damit als Indikator dafür, wie herausfordernd die Umsetzung der CRA-Vorgaben voraussichtlich ausfällt, insbesondere für KMU mit begrenzten Ressourcen.

Wie Abbildung 4-1: Cybersicherheitsrating nach BranchengruppenAbbildung 4-1 zeigt, belegen die mutmaßlich vom CRA betroffenen Branchengruppen Informations- und Kommunikationswirtschaft sowie Handel mit jeweils 706 Punkten die letzten Plätze im Cybersicherheitsrating. Die Industrie erreicht mit 716 Punkten ein etwas besseres Ergebnis, liegt aber dennoch nur im oberen Mittelfeld. Diese Werte deuten darauf hin, dass viele Unternehmen in CRA-relevanten Branchen vor erheblichen Umsetzungsaufgaben stehen: nicht nur in Bezug auf technische Produktanforderungen, sondern auch hinsichtlich interner Prozesse, Dokumentationsfähigkeit und Sicherheitskultur. Vor diesem Hintergrund rücken im CRA-Kontext mehrere strukturelle Herausforderungen in den Fokus, die für die praktische Umsetzung der Verordnung von zentraler Bedeutung sein dürften.

4.3.3 Zentrale Herausforderungen im Kontext des Cyber Resilience Acts

Herausforderungen für KMU im Kontext des CRA liegen weniger in der grundsätzlichen Einschätzung der Betroffenheit gemäß des CRA, denn für Hersteller von Produkten mit digitalen Elementen ist die Pflichtenlogik grundsätzlich klar. Sie folgt dem „New Legislative Framework" (NLF), dem horizontalen EU-Rahmenwerk für Produktregeln im Binnenmarkt.

Bis auf reine Softwarehersteller sollten die Hersteller von Produkten mit digitalen Elementen bereits von EU-Harmonisierungsvorschriften betroffen sein. Der CRA stellt somit keinen Strukturbruch dar, sondern eine horizontale Ergänzung. Er konkretisiert Cybersicherheitsanforderungen über die Bereitstellung hinaus in die Nutzungsphase. Neu ist insbesondere auch die Pflicht, Sicherheitsfunktionen über mindestens fünf Jahre bzw. die kürzere Produktlebensdauer aufrechtzuerhalten, sowie der Nachweis eines kontinuierlichen Schwachstellenmanagements, welches diese Aufrechterhaltung operativ absichert.

Praktische Unsicherheiten können entstehen, wenn Unternehmen zwischen Rollen in Bezug auf ein Produkt wechseln, beispielsweise wenn ein Händler durch eine Eigenmarke oder durch eine wesentliche Änderung des Produkts zum Hersteller wird. Unsicherheiten können auch bei Softwareanbietern entstehen, die mit Hybridmodellen arbeiten – zum Beispiel wenn fertige Software-Bausteine oder Entwicklerpakete (SDKs) in ein eigenes Produkt eingebaut werden, wenn es eine kostenlose Basisversion mit kostenpflichtigen Zusatzfunktionen gibt (Freemium), oder wenn offene Software mit einem kommerziellen Angebot kombiniert wird. In diesen Fällen ist oft nicht klar, wer am Ende für welche Teile verantwortlich ist: der ursprüngliche Hersteller des Bausteins oder das Unternehmen, das alles zusammenführt und an Kundinnen und Kunden ausliefert. Außerdem kann sich je nach Funktionsumfang ändern, welche Daten verarbeitet werden und welche Nachweise geführt werden müssen. Das macht es gerade für kleinere Unternehmen schwierig, ihre Pflichten eindeutig zu bestimmen und die Anforderungen verlässlich zu erfüllen.

Entlang der Lieferkette kann es für KMU zu Herausforderungen und Unsicherheiten kommen, wenn Pflichten wie Nachweisführung oder Schwachstellenmanagement faktisch weitergegeben werden. Für kleinere Softwareunternehmen und Einrichtungen im Bereich der Open-Source-Software markiert der CRA häufig den regulatorischen Einstieg (Kikelj/Sabic, 2024).

Die European Cyber Security Organisation (ECSO, 2022) fordert klare Methodiken zur Produktklassifizierung, um insbesondere KMU eine verlässliche Einordnung ihrer Verantwortlichkeiten zu ermöglichen. In ähnlicher Weise betont SMEunited (2022) die Notwendigkeit eindeutiger Vorgaben, etwa zur Haftung bei Cybervorfällen entlang der Lieferkette.

Insgesamt liegt die zentrale Herausforderung für KMU weniger in unklaren Rechtsbegriffen als in der Operationalisierung. Die Anforderungen an Risikoanalysen, technische Dokumentationen und kontinuierliches Schwachstellenmanagement bedeuten in vielen Unternehmen den Aufbau gänzlich neuer Kompetenzen und Prozesse. Wie bei der NIS-2-Richtlinie ist auch hier der Fachkräftemangel eine zentrale Hürde. Gefordert sind Fachkräfte, die sowohl regulatorisches Know-how als auch technisches Produktverständnis mitbringen und somit interdisziplinäre Schnittstellenrollen übernehmen – ein Profil, das am Markt bislang kaum verfügbar ist (vgl. SANS/GIAC, 2025). Die Folgen des Fachkräftemangels sind längere Time-to-Compliance, eine höhere Abhängigkeit von externen Dienstleistern, höhere Umsetzungskosten und Priorisierungsdruck bei Wartung und Updates. KMU konkurrieren insbesondere mit größeren Unternehmen um wenige verfügbare Fachkräfte. Besonders betroffen sind Branchen, in denen digitale Komponenten bislang nur eine untergeordnete Rolle spielten, die nun aber unter den Geltungsbereich des CRA fallen.

Eine weitere Herausforderung ist die geringe technologische und organisatorische Reife vieler KMU. Auch wenn diese über funktionierende Entwicklungs- und Produktionsprozesse verfügen, sind sie oft nicht auf kontinuierliche Cybersicherheitsbewertungen oder strukturierte Produktupdates ausgelegt. Dies gilt insbesondere für eingebettete Software in industriellen Produkten, für die bislang keine systematische Softwarepflege oder Update-Strategie implementiert worden ist.

Auch Händler und Einführer stehen vor neuen Herausforderungen. Obwohl sie häufig keine originäre technische Verantwortung für Produkte übernehmen, verlangt der CRA von ihnen umfangreiche Sorgfaltspflichten – etwa bei der Kontrolle von Dokumentation, CE-Kennzeichnung und der Weiterleitung sicherheitsrelevanter Informationen. Diese Prozesse sind in vielen Handelsunternehmen bislang nicht etabliert und müssen erst aufgebaut werden (ISMS.online, 2024).

Insgesamt erfordert der CRA von vielen KMU spürbare Anpassungen – sowohl in der technischen Produktentwicklung als auch in der regulatorischen Compliance. Besonders für kleinere Unternehmen, die erstmals reguliert werden und zudem noch über eine schwache IT-Infrastruktur verfügen, ist diese Umstellung mit hohem Aufwand verbunden.

4.3.4 Kosten im Kontext des Cyber Resilience Acts

Die Umsetzung des CRA verursacht sowohl einmalige Implementierungskosten als auch laufende Betriebskosten. Die Hauptlast tragen dabei die Hersteller digitaler Produkte. Nach Einschätzung der Europäischen Kommission entfällt der Großteil der Kosten auf den einmaligen Anpassungsaufwand – im Verhältnis von etwa 70 zu 30 gegenüber den laufenden Kosten (European Commission, 2022). Investitionen sind insbesondere erforderlich für den Aufbau sicherer Entwicklungsprozesse (Secure Development Lifecycle, SDLC), die Etablierung interner Prüfmechanismen sowie für externe Zertifizierungen.

Neben dem initialen Erfüllungsaufwand entstehen dauerhafte Kosten, um die CRA-Sicherheitsanforderungen über den gesamten Produktlebenszyklus hinweg zu erfüllen. Dazu zählen regelmäßige Sicherheitsupdates, die kontinuierliche Überwachung von Produkten auf neue Schwachstellen, die Meldepflichten an die Behörden sowie die Aktualisierung der technischen Dokumentation.

Insgesamt rechnet die Europäische Kommission mit EU-weiten CRA-bezogenen Kosten von 29 Milliarden Euro für die Unternehmen. Eine Aufschlüsselung der Kosten pro Unternehmen ist aufgrund der begrenzten Datenlage schwierig. Das Impact Assessment der Europäischen Kommission nimmt vereinfachend an, dass ein Unternehmen durchschnittlich ein digitales Produkt herstellt und dass die Entwicklungskosten pro Produkt bei rund 140.000 Euro liegen (European Parliament, 2022). Um die CRA-Anforderungen zu erfüllen, müssten die Entwicklungsausgaben durchschnittlich um 30 Prozent steigen, also um etwa 42.000 Euro pro Produkt. Dieser Wert umfasst sowohl den Initialaufwand als auch die laufenden Betriebskosten über den gesamten Lebenszyklus.

Die tatsächliche Belastung hängt jedoch stark vom jeweiligen Ausgangsniveau ab. Unternehmen, die bereits nach dem Prinzip Security by Design arbeiten oder bestehende sicherheitsrelevante Normen umsetzen, haben geringere Zusatzaufwände. Ein IT-Start-up, das Sicherheitsaspekte bisher vernachlässigt hat, könnte demgegenüber erstmals fünfstellige Summen in sichere Entwicklungsprozesse investieren müssen.

Besonders KMU sind durch den CRA gefordert. Sie verfügen häufig nicht über interne Kapazitäten in den Bereichen IT-Sicherheit oder Produktsicherheit und müssen daher auf externe Beratung und Prüfung zurückgreifen. Skaleneffekte, wie sie große Unternehmen bei der Umsetzung geltend machen können, fehlen (European Commission, 2022). Dementsprechend kann der CRA bei KMU nicht nur zu erheblichen Mehraufwendungen führen, sondern auch andere Investitionen verdrängen. Mehrere Branchenverbände warnten im Konsultationsprozess vor einer möglichen Marktverdrängung kleiner Anbieter durch überhöhte Compliance-Kosten (ebd.).

Auch Einführer und Händler müssen mit zusätzlichen Belastungen rechnen. Zwar gelten ihre Pflichten als weniger umfangreich als jene der Hersteller und können vielfach in bestehende Prozesse integriert werden – etwa bei der Prüfung der technischen Dokumentation oder der CE-Kennzeichnungen. Doch gerade kleinere Handelsunternehmen, die über keine eigene Rechts- oder Compliance-Abteilung verfügen, sind auf externe Unterstützung angewiesen. Das gilt insbesondere für Unternehmen, die mit außereuropäischen Anbietern zusammenarbeiten.

Hinzu kommen mögliche Zusatzkosten für mittelbar betroffene Unternehmen, etwa Zulieferer von Hard- oder Softwarekomponenten. Auch wenn sie formal nicht zu den Primäradressaten des CRA zählen, müssen sie im Rahmen von Lieferbeziehungen sicherheitsrelevante Informationen, Nachweise oder vertragliche Zusicherungen bereitstellen. Die Höhe dieser mittelbaren Belastungen ist bislang nicht offiziell geschätzt worden und dürfte stark vom Geschäftsmodell sowie vom Grad der Integration in regulierte Lieferketten abhängen.

4.3.5 Nutzen des Cyber Resilience Acts

Trotz der spürbaren Umsetzungskosten, insbesondere für KMU, bietet der CRA mittel- bis langfristig erhebliche Vorteile. Ziel des CRA ist es, die Sicherheit digitaler Produkte systematisch zu erhöhen und damit eine vertrauenswürdige und belastbare digitale Produktlandschaft im europäischen Binnenmarkt zu schaffen. Er schließt eine bisherige Regulierungslücke: Bislang existierten keine harmonisierten Mindestanforderungen an die Cybersicherheit von Produkten mit digitalen Elementen, insbesondere nicht über mehrere Jahre beziehungsweise die gesamte Produktlebensdauer hinweg.

Durch einheitliche Sicherheitsanforderungen verbessert der CRA die technische Qualität digitaler Produkte, reduziert Schwachstellen bereits in der Entwicklungsphase und fördert die kontinuierliche Pflege durch Updates. Daraus ergibt sich eine geringere Anfälligkeit gegenüber Cyberangriffen und damit eine potenzielle Reduktion von wirtschaftlichen Schäden durch Ausfälle, Betriebsunterbrechungen, Datenverlust oder Reputationsschäden. So ist damit zu rechnen, dass es insgesamt weniger Cybersicherheitsvorfälle gibt (European Commission, 2025).

Wie im Impact Assessment (European Commission, 2022) betont, wirkt der CRA zudem marktordnend: Er schafft einheitliche Wettbewerbsbedingungen, weil durch ihn alle Marktteilnehmer innerhalb der EU denselben Sicherheitsvorgaben unterliegen. Das stärkt den fairen Wettbewerb, verhindert Marktverzerrungen durch Billiganbieter mit niedrigen Sicherheitsstandards und verbessert die Vergleichbarkeit von Produkten. Hersteller, die hohe Sicherheitsstandards einhalten, können sich durch dokumentierte Konformität künftig besser im Markt positionieren. Das steigert nicht nur die Produktqualität, sondern auch das Vertrauen von Geschäftspartnern und Endkunden sowohl innerhalb als auch außerhalb der EU. Der CRA wird dazu führen, dass die Nachfrage nach Produkten mit transparenten Cybersicherheitseigenschaften steigt (Arzt et al., 2025).

Besonders für international tätige Unternehmen bietet der CRA zudem die Chance, frühzeitig regulatorische Konformität mit künftigen globalen Sicherheitsstandards zu erreichen. Die EU nimmt mit dem CRA eine Vorreiterrolle ein, sodass mit der Zeit auch außereuropäische Märkte ähnliche Anforderungen einführen dürften (Mueck et al., 2023). Hersteller, die bereits CRA-konform entwickeln, sichern sich damit weltweite Marktzugänge.

Nicht zuletzt kann die strukturierte Auseinandersetzung mit Cybersicherheit im Produktkontext positive Rückwirkungen auf unternehmensinterne Prozesse haben – insbesondere bei kleinen und mittleren Unternehmen, die bislang kaum Berührungspunkte mit IT-Sicherheit hatten. Der CRA fördert eine systematische Dokumentation, klare Verantwortlichkeiten und ein stärkeres Bewusstsein für Risiken entlang des Produktlebenszyklus. Dadurch steigt auch die organisationsinterne Resilienz gegenüber sicherheitskritischen Vorfällen.

Insgesamt trägt der CRA somit dazu bei, die digitale Produktlandschaft in Europa nachhaltiger, sicherer und wettbewerbsfähiger zu gestalten – mit entsprechenden Vorteilen für Wirtschaft und Gesellschaft.

4.4 Unterstützungsbedarfe der KMU

Die Analyse der Betroffenheit und Herausforderungen im Kontext von NIS-2-Richtlinie und CRA zeigt: Viele zehntausende KMU in Deutschland stehen vor komplexen regulatorischen Anforderungen im Bereich Cybersicherheit – sowohl in Bezug auf ihre betriebliche IT als auch auf ihre digitalen Produkte. Insbesondere Unternehmen ohne eigene IT-Abteilung oder Compliance-Strukturen

benötigen gezielte Unterstützung, um ihre neuen Pflichten rechtskonform und effizient umzusetzen. Die Unterstützungsbedarfe der KMU lassen sich – wie auch schon bei der KI-Verordnung – drei zentralen Dimensionen zuordnen:

- Informationsbedarf: Viele KMU wissen nicht, ob sie von den neuen Regelungen betroffen sind oder welche Pflichten sich daraus konkret ergeben. Dies gilt insbesondere für Unternehmen mit Misch- oder Zuliefertätigkeiten, die nicht eindeutig einem NIS-2-Sektor zugeordnet werden können oder deren Produktrollen im Sinne des CRA unklar sind. Entsprechend groß ist der Bedarf an verständlichen, adressatengerechten und rechtssicheren Orientierungshilfen – idealerweise gebündelt, um eine Überforderung durch die Vielzahl paralleler Informationsquellen zu vermeiden.
- Kompetenzbedarf: Technische Schutzmaßnahmen, organisatorisches Risikomanagement und Dokumentationspflichten erfordern Know-how, das in vielen KMU nicht vorhanden ist. Schulungen und praxisnahe Unterstützung sind daher essenziell – insbesondere in Bereichen wie Schwachstellenmanagement, ISMS-Aufbau oder sicherheitskonformer Produktentwicklung.
- Ressourcenbedarf: Die Erfüllung regulatorischer Pflichten bindet personelle und finanzielle Mittel. Viele KMU benötigen daher nicht nur Wissen, sondern auch Zugang zu passenden Tools, Fördermitteln und externer fachlicher Unterstützung.

Die Wirksamkeit von Unterstützungsangeboten hängt dabei maßgeblich von ihrer Passgenauigkeit ab. Viele KMU benötigen Formate, die spezifisch auf ihre Branche, ihre Rolle in der Lieferkette und ihre regulatorische Betroffenheit zugeschnitten sind. Gerade bei stark differenzierten Anforderungen wie denen des CRA oder der NIS-2-Richtlinie ist ein hohes Maß an Spezifizierung erforderlich, um Unternehmen nicht nur zu sensibilisieren, sondern tatsächlich zur Umsetzung zu befähigen.

4.4.1 Bestehende Angebote

In Deutschland existiert eine Vielzahl an Unterstützungsangeboten, die KMU beim Aufbau von Cybersicherheitskompetenzen begleiten. Besonders hervorzuheben sind das Netzwerk der Mittelstand-Digital Zentren und die Initiative IT-Sicherheit in der Wirtschaft. Die regional, branchenspezifisch oder thematisch ausgerichteten Mittelstand-Digital Zentren bieten kostenfreie und anbieterneutrale Informationen, Veranstaltungen, Schulungen und weitere Unterstützungsangebote auch zum Thema Cybersicherheit an.

Die im Rahmen der Initiative IT-Sicherheit in der Wirtschaft geförderte Transferstelle Cybersicherheit im Mittelstand (CYBERsicher) steht zudem als zentrale Anlaufstelle speziell zum Thema Cybersicherheit zur Verfügung und arbeitet eng mit den Mittelstand-Digital Zentren zusammen. Sie bietet beziehungsweise vermittelt Unterstützung in Form von digitalen Tools und Materialien, wie dem CYBERsicher-Check zur Einschätzung des betrieblichen Sicherheitsniveaus (https://transferstelle-cybersicherheit.de/cybersicher-check/), Leitfäden zu organisatorischen und technischen Maßnahmen, eine Notfallhilfe, sowie die ISMS-Werkstatt mit modularen Workshops zum Aufbau eines Informationssicherheits-Managementsystems (https://transferstelle-cybersicherheit.de/die-isms-werkstatt/). Die Transferstelle verbreitet zudem Tools und Unterstützungsmaterialien, die durch weitere Projekte aus der Initiative IT-Sicherheit in der Wirtschaft erarbeitet wurden. Beispiele dafür sind der FitNIS2-Navigator oder die gamifizierten Lernangebote von BAKSecure (https://baksecure.de/). Der FitNIS2-Navigator bietet eine strukturierte Betroffenheitsprüfung zur NIS-2-Richtlinie und unterstützt Unternehmen bei der Ableitung konkreter Handlungsbedarfe (https://fitnis2.de/selbstpruefung/). Ebenfalls von der Transferstelle verbreitet wird das praxisnahe Unterstützungsangebot KMU.kompetent.sicher. (https://kmu-kompetent-sicher.de/; Laufzeit: November 2024 bis Oktober 2027). Ziel ist die Entwicklung einer modularen NIS-2-Test- und Trainingsplattform, die KMU befähigt, ihre IT-Sicherheit auf das geforderte Niveau der NIS-2-Richtlinie zu bringen.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) bietet ebenfalls zahlreiche Informationsangebote an, darunter die bereits erwähnte NIS-2-Betroffenheitsprüfung. Außerdem hat

das BSI im September 2025 eine Handreichung für die Empfehlung zur Schulungspflicht für Geschäftsleitungen im Rahmen von NIS-2 veröffentlicht. Auf der Plattform der Allianz für Cyber-Sicherheit (https://www.allianz-fuer-cybersicherheit.de/) finden Unternehmen Informationsangebote wie Webinare, Checklisten und Vorlagen. Für Hersteller digitaler Produkte hat das BSI technische Richtlinien (z. B. BSI TR-03183) veröffentlicht, die als erste Orientierung zur CRA-Umsetzung dienen können (BSI, 2024). Erwartet wird zudem, dass das BSI künftig eine koordinierende Funktion als nationaler One-Stop-Shop einnimmt, der Unternehmen sowohl bei NIS-2 als auch beim CRA unterstützt.

Darüber hinaus stellen auch viele Bundesländer eigene Unterstützungsangebote bereit – etwa Leitfäden und Beratungsinitiativen. Über Förderprogramme wie „Förderung von Unternehmensberatungen für KMU", den ERP-Förderkredit Digitalisierung oder landesspezifische Förderungen wie die Digitalisierungsfinanzierung Baden-Württemberg können Beratungsleistungen und Investitionen in IT-Sicherheit finanziell unterstützt werden.

Auf europäischer Ebene unterstützten Programme wie Horizon Europe und Digital Europe KMU vor allem beim Kompetenzaufbau, der technologischen Erprobung und Pilotierung im Bereich IT-Sicherheit, nicht jedoch bei der Umsetzung konkreter Compliance-Pflichten. Als Teil des Förderprogramms Digital Europe fungieren die European Digital Innovation Hubs (EDIHs) als regionale Anlaufstellen, die KMU sowie öffentliche Einrichtungen bei der Einführung digitaler Technologien unterstützen. Viele deutsche EDIHs bieten direkt oder indirekt Unterstützung im Bereich IT-Sicherheit, etwa über Testeinrichtungen, Schulungsprogramme, Beratung oder Entwicklungsleistung. Hubs wie der European Digital Innovation Hub Applied Artificial Intelligence and Cybersecurity (AICS) in Baden-Württemberg oder der niedersächsische European Digital Innovation Hub for AI & Cybersecurity (DAISEC) setzen gezielt auf Cybersicherheit als Schlüsselelement ihres Angebots.

Auch die EU-Cybersicherheitsagentur ENISA bietet Leitfäden, Tools und Pilotprogramme zur Unterstützung.

Insgesamt ergibt sich ein dichtes Netz an Informations- und Unterstützungsformaten. Viele Unternehmen verharren trotz diesen Angebots in einer passiven Haltung. Dabei dürften Unsicherheit, fehlende Umsetzungsfähigkeit und Überforderung eine Rolle spielen. Auch die Vielfalt der Angebote kann bei KMU zu Verunsicherung führen, wenn Inhalte unkoordiniert nebeneinanderstehen. Um die Gefahr der Überforderung zu reduzieren und die Wirksamkeit zu steigern, sollte insgesamt stärker auf Koordination, Transparenz und klare Zielgruppenorientierung geachtet werden.

4.4.2 Empfehlungen für die Weiterentwicklung der Angebote

Um die Compliance der KMU mit der neuen Cybersicherheitsregulierung zu vereinfachen und vor allem ihre Cybersicherheit zu stärken, sollten bestehende Angebote gezielt entlang der oben genannten Bedarfsdimensionen ausgebaut und systematisch weiterentwickelt werden. Folgende Empfehlungen ergeben sich aus der Analyse:

- Branchenspezifische Unterstützungsformate ausbauen und auf Regulierung ausrichten: Leitfäden, Praxisbeispiele und Tools sollten gezielt für besonders betroffene Branchen und Regulierungsadressaten entwickelt werden – etwa Maschinenbau, Gesundheitswesen, Logistik oder Hersteller von Produkten mit digitalen Elementen. Die Initiative Cybersicherheit im Handwerk des Mittelstand-Digital Zentrums Handwerk (https://cybersicherheit-handwerk.de/) kann dabei als Vorbild dienen, sollte aber noch deutlich stärker auf NIS-2 und CRA ausgerichtet werden.
- CRA-Readiness-Check und Umsetzungstool einführen: Analog zum FitNIS2-Navigator wäre empfehlenswert, ein CRA-spezifisches Tool zu entwickeln, das Unternehmen bei der Umsetzungsplanung unterstützt – inklusive Dokumentationsvorlagen und Förderinformationen.

- Förderberatung systematisch integrieren: Bestehende Angebote wie der FitNIS2-Navigator oder die ISMS-Werkstatt könnten automatisiert aktive Förderoptionen einbinden und idealerweise eine direkte Unterstützung bei der Antragstellung anbieten. So können Ressourcenbarrieren abgebaut und Investitionsentscheidungen beschleunigt werden.
- Zugang zu qualifizierter externer Unterstützung verbessern: Viele KMU benötigen konkrete Hilfe bei Umsetzung und Auditvorbereitung. Eine zentrale Beratungsplattform oder ein IT-Sicherheitslotsen-Programm könnte schnell und transparent Zugang zu qualifizierten Fachkräften schaffen – regional vernetzt, qualitätsgesichert und branchennah.
- Formate auf Umsetzungsergebnisse ausrichten: Unterstützungsangebote sollten stärker auf konkrete Outputs abzielen – z. B. ISMS-Dokumentation, Umsetzungskits für NIS-2, Auditvorbereitung oder CE-Kennzeichnung im CRA-Kontext. Die bestehende ISMS-Werkstatt ist ein wertvoller Ansatz, der um branchenspezifische Inhalte und CRA-relevante Module erweitert werden sollte.

Bestehende Formate wie der FitNIS2-Navigator zeigen bereits, dass Befähigung und praktische Umsetzung zentrale Bestandteile erfolgreicher Unterstützungsangebote sind. Durch eine systematische Weiterentwicklung und stärkere Verzahnung der Angebote können KMU künftig noch gezielter dabei unterstützt werden, regulatorische Vorgaben wie NIS-2 und den Cyber Resilience Act praktisch und ressourcenschonend umzusetzen und damit ihre digitale Resilienz und Wettbewerbsfähigkeit nachhaltig zu stärken.

5. Ausblick

Die Analyse hat gezeigt, dass zahlreiche KMU in Deutschland in erheblichem Maße von den neuen Regulierungen – der KI-Verordnung, der NIS-2-Richtlinie und dem Cyber Resilience Act – betroffen sind. Die regulatorischen Anforderungen sind komplex und setzen häufig ein Niveau an organisatorischen, technischen und rechtlichen Kompetenzen voraus, das in vielen KMU bislang nicht vorhanden ist – auch, weil viele Unternehmen erstmals regulatorisch adressiert werden. Gleichzeitig laufen die Umsetzungsfristen, und einzelne Vorschriften sind bereits anzuwenden.

Vor diesem Hintergrund ist es entscheidend, dass Unternehmen sich frühzeitig und systematisch mit den neuen Pflichten auseinandersetzen. Wer erst kurz vor oder sogar nach Ablauf der Fristen reagiert, riskiert nicht nur hohe Compliance-Kosten und sogar Sanktionen, sondern auch Wettbewerbsnachteile. Die Zeit drängt – sowohl, weil der regulatorische Rahmen verbindlich wird, als auch, weil Cybersicherheit und der vertrauenswürdige Einsatz von KI längst zentrale Faktoren unternehmerischer Resilienz und Wettbewerbsfähigkeit sind.

Die Umsetzung der Vorgaben sollte daher nicht als reine Pflichtaufgabe verstanden werden, sondern als strategische Investition: Eine robuste Cyber- und KI-Sicherheitsarchitektur erhöht nicht nur die Rechtssicherheit, sondern schützt auch vor finanziellen Verlusten, Reputationsschäden und operativen Ausfällen. Sie kann zudem neue Marktchancen eröffnen, etwa durch den Zugang zu sicherheitskritischen Aufträgen oder die Erschließung regulierter Märkte.

Darüber hinaus trägt die Fähigkeit, digitale Technologien sicher, vertrauenswürdig und regelkonform einzusetzen, maßgeblich zur digitalen Souveränität bei – sowohl auf Ebene der einzelnen Unternehmen als auch im gesamtwirtschaftlichen Kontext. Unternehmen, die ihre digitalen Infrastrukturen, Daten und KI-Anwendungen unter Kontrolle haben, reduzieren Abhängigkeiten von unsicheren oder unzuverlässigen Drittanbietern. Das stärkt die wirtschaftliche Handlungsfähigkeit Europas und seine Unabhängigkeit in geopolitisch sensiblen Technologiebereichen.

Damit dieser Wandel gelingt, müssen KMU in die Lage versetzt werden, regulatorische Anforderungen effizient und ressourcenschonend umzusetzen. Das erfordert unter anderem eine umsetzungsorientierte Unterstützung, branchenspezifische Angebote, die klare Kommunikation von

Pflichten und Fristen sowie den schnellen Ausbau der regulatorisch vorgesehenen Entlastungsinstrumente.

Je eher Unternehmen den Transformationsprozess beginnen, desto besser können sie regulatorische Risiken minimieren, Kosten kontrollieren und den technologischen Wandel aktiv gestalten. Besser gestern als heute gilt hier nicht nur mit Blick auf die Fristen – sondern auch, weil eine starke Cyber- und KI-Sicherheitskultur ein entscheidender Wettbewerbsvorteil der Zukunft und ein Fundament für die digitale Souveränität Europas sein wird.

Literaturverzeichnis

AI Quality & Testing Hub, 2025, Künstliche Intelligenz auf dem Prüfstand, https://aiqualityhub.com/ [7.10.2025]

Arroyabe, Marta F. / Arranz, Carlos D.A. / De Arroyabe, Ignacio, F. / De Arroyabe, Juan Carlos F., 2024, Exploring the economic role of cybersecurity in SMEs: A case study of the UK, Technology in Society, 78. Jg., 102670

Arzt, Steven / Fischer, Leonie / Kreutzer, Michael / Scheel, Kirstin / Schneider, Markus / Schreiber, Linda / Selzer, Annika, 2025, Der EU Cyber Resilience Act: Ein Überblick aus rechtlicher Sicht, https://www.sit.fraunhofer.de/fileadmin/dokumente/studien_und_technical_reports/CRA-Recht_202504.pdf?_=1741789240 [7.10.2025]

Bayrisches Staatsministerium für Digitales, 2025, KMUs bei der Umsetzung des „AI Act" der EU unterstützen // Bayern zum Vorreiter für verantwortungsvolle KI machen // Mehring: „Wir spannen Schutzschirm vor EU Bürokratie über Bayerns Wirtschaft auf", Pressemitteilung vom 30. Januar 2025, https://www.stmd.bayern.de/kmus-bei-der-umsetzung-des-ai-act-der-eu-unterstuetzen-bayern-zum-vorreiter-fuer-verantwortungsvolle-ki-machen-mehring-wir-spannen-schutzschirm-vor-eu-buerokratie-ue/ [7.10.2025]

Bitkom, 2025a, Wirtschaftsschutz 2025, https://www.bitkom.org/sites/main/files/2025-09/bitkom-pressekonferenz-wirtschaftsschutz-cybercrime.pdf [7.10.2025]

Bitkom, 2025b, Ein Fünftel wurde im Job zu KI geschult, https://www.bitkom.org/print/pdf/node/24611 [7.10.2025]

Bitkom, 2024a, Jedes vierte Unternehmen beschäftigt sich mit dem AI Act, https://www.bitkom.org/print/pdf/node/22131 [7.10.2025]

Bitkom, 2024b, Mangel an IT-Fachkräften droht sich dramatisch zu verschärfen, https://www.bitkom.org/Presse/Presseinformation/Mangel-an-IT-Fachkraeften-droht-sich-zu-verschaerfen [7.10.2025]

Büchel, Jan / Engels, Barbara, 2025, Cybersicherheit: Kompetenzen gefragter denn je, IW-Kurzbericht, Nr. 39, Köln

Büchel, Jan / Engler, Jan Felix, 2024, Generative KI in Deutschland. Künstliche Intelligenz in Gesellschaft und Unternehmen, IW-Report, Nr. 23, Köln, https://www.iwkoeln.de/fileadmin/user_upload/Studien/Report/PDF/2024/IW-Report_2024-Generative-KI-in-Deutschland.pdf [7.10.2025]

Büchel, Jan / Engler, Jan Felix / Mertens, Armin, 2025, KI-Jobs in Deutschland: Stagnation statt Boom. Eine Analyse von Online-Stellenanzeigen, Studie im Auftrag der Bertelsmann Stiftung (Hrsg.), Gütersloh

BSI – Bundesamt für Sicherheit in der Informationstechnik, 2024, Technical Guideline TR-03183: Cyber Resilience Requirements for Manufacturers and Products – Part 2: Software Bill of Materials (SBOM) Version 2.0.0, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TR03183/BSI-TR-03183-2-2_0_0.pdf?__blob=publicationFile&v=3f [7.10.2025]

Budde, Klemens, Hiltawsky, Karsten et al. (2025): KI-Verordnung: Ihre Auswirkungen für Medizinprodukte. Herausforderungen und offene Fragen. Impulspapier aus der Plattform Lernende Systeme, München. DOI: https://doi.org/10.48669/pls_2025-4 [8.10.2025]

Bundesamt für Sicherheit in der Informationstechnik (BSI), 2025a, Entscheidungsbaum der NIS-2-Betroffenheitsprüfung des BSI, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/NIS-2/nis-2-betroffenheit-entscheidungsbaum.html [7.10.2025]

Bundesamt für Sicherheit in der Informationstechnik (BSI), 2025b, Cyber Resilience Act, https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Cyber_Resilience_Act/cyber_resilience_act_node.html [7.10.2025]

Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BFDI), 2025, Pilotprojekt KI-Reallabor, https://www.bfdi.bund.de/SharedDocs/Kurzmeldungen/DE/2025/09-KI-Reallabor.html [7.10.2025]

Bundesnetzagentur, 2025, KI-Service-Desk, https://www.bundesnetzagentur.de/DE/Fachthemen/Digitales/KI/start_ki.html [7.10.2025]

Bundesministerium des Innern (BMI), 2025, Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (Referentenentwurf), https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/Downloads/referentenentwuerfe/CI1/NIS-2-RefE_2025.pdf?__blob=publicationFile&v=9 [7.10.2025]

Bundesverband der Deutschen Industrie (BDI), 2024, Zur Durchführung von EU-AI Act und EU Data Act (Position), https://bdi.eu/publikation/news/zur-durchfuehrung-von-eu-ai-act-und-eu-data-act [7.10.2025]

Bundesvereinigung der Deutschen Arbeitgeberverbände (BDA), 2024, EU AI Act – Was steht drin? https://arbeitgeber.de/wp-content/uploads/2024/11/bda-arbeitgeber-regelung_ki_verordnung-EU_AI_Act-was_steht_drin-2024-11.pdf [7.10.2025]

CEN / CENELEC / ETSI, 2025, Standardization in support of the EU Cyber Resilience Act, https://www.stan4cra.eu/ [7.10.2025]

Chiara, Pier Giorgio, 2025, Understanding the Regulatory Approach of the Cyber Resilience Act: Protection of Fundamental Rights in Disguise?, in: European Journal of Risk Regulation, 16. Jg., Nr. 2, S. 469–484

Cloudflare, 2025, Von 20,5 Millionen DDoS-Angriffen betroffen, ein Anstieg um 358 % im Jahresvergleich: Der Cloudflare-Bericht zur DDoS-Bedrohungslandschaft für das erste Quartal 2025, https://blog.cloudflare.com/de-de/ddos-threat-report-for-2025-q1/ [7.10.2025]

Datenschutzkonferenz, 2025, Orientierungshilfe zu empfohlenen technischen und organisatorischen Maßnahmen bei der Entwicklung und beim Betrieb von KI-Systemen. Version 1.0, https://www.datenschutzkonferenz-online.de/media/oh/DSK-OH_KI-Systeme.pdf [7.10.2025]

Davallas, Athanasios / Angelaki, Anna / Beretas, Christos P., 2025, Compliance or Innovation? The Balancing Act for Startups Under the AI Act, https://www.researchgate.net/publication/388724045_Compliance_or_Innovation_The_Balancing_Act_for_Startups_Under_the_AI_Act [7.10.2025]

Deloitte, 2024, Umfrage AI Act 2024 – Befragung zu den Auswirkungen des AI Acts, https://www.deloittelegal.de/content/dam/assets-zone6/dl/de/docs/services/legal/2025/Deloitte_AI-Act-Umfrage-Sep2024.pdf [07.10.2025]

Demary, Vera / Grömling, Michael / Kestermann, Christian / Scheufen, Marc / Seele, Stefanie / Stettes, Oliver / Trenz, Marco, 2025, Wie wird KI die Produktivität in Deutschland verändern?, Gutachten im Auftrag des Gemeinschaftsausschusses der Deutschen Gewerblichen Wirtschaft, Köln / Berlin

Deutscher Bundestag, 2024, Wortprotokoll der 90. Sitzung – Ausschuss für Inneres und Heimat, https://www.bundestag.de/resource/blob/1038526/8c8839889e7d24c95f7a2cfb0e0cf440/Protokoll-04-11-2024-11-00-Uhr.pdf [7.10.2025]

DIN, 2023, DIN SPEC 27076:2023-05, https://www.dinmedia.de/de/technische-regel/din-spec-27076/365252629 [7.10.2025]

ECSO, 2022, POSITION PAPER Cyber Resilience Act, https://ecs-org.eu/ecso-uploads/2023/01/ECSO_position_on_the_CRA.02.pdf [7.10.2025]

Eger, Thomas / Scheufen, Marc, 2024, Data Sharing in Deutschland. Theorie, Empirie und europäische Gesetzgebung, in: Wirtschaftsdienst, 104. Jg., Heft 10, S. 725–729

Engels, Barbara / Scheufen, Marc / Schmitz, Edgar, 2025, Künstliche Intelligenz als Wettbewerbsfaktor für die deutsche Wirtschaft. Empirische Befunde und Handlungsempfehlungen zum Einsatz von KI in deutschen Unternehmen, IW-Report, Nr. 33, Köln

ENX Association, 2025, TISAX and Cybersecurity in Industry – Expert Analysis Confirms NIS2 Coverage, https://enx.com/en-US/news/TISAX-NIS2/ [7.10.2025]

Europäische Kommission, 2021, Commission Staff Workung Dokument – Impact Assessment Accompanying the Proposal for a Regulation of the European Parliament and of the Council, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52021SC0084 [7.10.2025]

Europäische Kommission, 2025a, NIS-2-Richtlinie: Neue Vorschriften für die Cybersicherheit von Netz- und Informationssystemen, https://digital-strategy.ec.europa.eu/de/policies/nis2-directive [7.10.2025]

Europäische Kommission, 2025b, Sectorial AI Testing and Experimentation Facilities under the Digital Europe Programme, https://digital-strategy.ec.europa.eu/en/policies/testing-and-experimentation-facilities [7.10.2025]

Europäische Kommission, 2025c, In Deutschland entsteht zweite europäische KI-Fabrik, https://germany.representation.ec.europa.eu/news/deutschland-entsteht-zweite-europaische-ki-fabrik-2025-03-12_de [7.10.2025]

European Commission, 2022, COMMISSION STAFF WORKING DOCUMENT – IMPACT ASSESSMENT REPORT – Annexes to the Impact Assessment Report Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020, Brüssel

European Parliament, 2022, Strengthening cyber resilience – Initial Appraisal of a European Commission Impact Assessment, https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/734708/EPRS_BRIE_APIN_734708_Cyber_resilience_final.pdf [7.10.2025]

EU, 2022a, Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union (NIS-2-Richtlinie), Amtsblatt der Europäischen Union, L 317/1 vom 27. Dezember 2022, https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022L2555 [7.10.2025]

EU, 2022b, Verordnung (EU) 2022/1925 des Europäischen Parlaments und des Rates vom 14. September 2022 über bestreitbare und faire Märkte im digitalen Sektor und zur Änderung der Richtlinien (EU) 2019/1937 und (EU) 2020/1828 (Gesetz über digitale Märkte). Amtsblatt der Europäischen Union, L 265 vom 12.10.2022, https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022R1925 [7.10.2025]

EU, 2022c, Verordnung (EU) 2022/2065 des Europäischen Parlaments und des Rates vom 19. Oktober 2022 über einen Binnenmarkt für digitale Dienste und zur Änderung der Richtlinie 2000/31/EG (Gesetz über digitale Dienste). Amtsblatt der Europäischen Union, L 277 vom 27.10.2022, https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022R2065 [7.10.2025]

EU, 2023, Verordnung (EU) 2023/2854 des Europäischen Parlaments und des Rates vom 13. Dezember 2023 über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung sowie zur Änderung der Verordnung (EU) 2017/2394 und der Richtlinie (EU) 2020/1828

(Datenverordnung). Amtsblatt der Europäischen Union, L vom 22.12.202, https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=OJ:L_202302854 [7.10.2025]

EU, 2024a, Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. März 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung der Verordnungen (EU) 2022/2065 und (EU) 2023/2854 sowie der Richtlinie (EU) 2020/1828 (KI-Verordnung). Amtsblatt der Europäischen Union, L 1689 vom 12.06.2024, S. 1–219, https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=OJ:L_202401689 [7.10.2025]

EU, 2024b, Verordnung (EU) 2024/2847 des Europäischen Parlaments und des Rates vom 13. März 2024 über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen und zur Änderung der Verordnung (EU) 2019/1020, ABl. L 2024/2847 vom 11.6.2024, S. 1–93, https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=OJ:L_202402847 [7.10.2025].

European Union Agency for Cybersecurity (ENISA), 2025, Technical Implementation Guidance, https://www.enisa.europa.eu/sites/default/files/2025-06/ENISA_Technical_implementation_guidance_on_cybersecurity_risk_management_measures_version_1.0.pdf [7.10.2025]

Eurostat (2025), Künstliche Intelligenz, nach Unternehmensgrößenklasse, https://ec.europa.eu/eurostat/databrowser/view/isoc_eb_ai__custom_18215533/default/table [7.10.2025]

Ferner, Jens, 2024, Konformität von KI-Systemen, in: PB Praxis Beschäftigungsdatenschutz, https://www.iww.de/pb/digitalisierung-ki/digitalisierung-ki-konformitaet-von-ki-systemen-f163414 [7.10.2025]

Fortinet, 2024, 2024 Cybersecurity Skills Gap – Global Research Report, https://www.fortinet.com/content/dam/fortinet/assets/reports/2024-cybersecurity-skills-gap-report.pdf [7.10.2025]

Ganser, Oliver / Reich, Christina, 2025, FOM VerhaltensRadar: Einstellungen, Chancen und Risiken der Künstlichen Intelligenz in Deutschland. FOM Sommerstudie 2025 – Ergebnisse, https://forschung.fom.de/uploads/forschungsprojekte/downloads/FOM-ifes-KI-Einstellungen-VerhaltensRadar-Deutschland-2025.pdf [8.10.2025]

Haataja, Meerie / Bryson, Joanna J., 2021, What costs should we expect from the EU's AI Act?, https://www.researchgate.net/profile/Joanna-Bryson/publication/354171430_What_costs_should_we_expect_from_the_EU's_AI_Act/links/64356bca609c170a130cea84/What-costs-should-we-expect-from-the-EUs-AI-Act.pdf?_tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6InB1YmxpY2F0a [7.10.2025]

Hessel, Stefan, 2025, Das neue Cybersicherheitsrecht der EU – Auswirkungen von NIS-2 und CRA auf den Datenschutz, https://stiftungdatenschutz.org/veranstaltungen/unsere-veranstaltungen-detailansicht/cybersicherheitsrecht-der-eu-543#c5914 [7.10.2025]

Industrie- und Handelskammer Köln (IHK Köln), 2025, Zertifikatslehrgänge – KI-Kompetenzpflicht 2025: Schulung zur KI-Verordnung und AI-Act, https://www.ihk.de/koeln/hauptnavigation/weiterbildung/zertifikatslehrgaenge/ki-kompetenzpflicht-2025-schulung-zur-ki-verordnung-und-ai-act-6494802 [7.10.2025]

IHK München und Oberbayern – Industrie- und Handelskammer München und Oberbayern, 2025, Artificial Intelligence Act – das müssen Unternehmen wissen, https://www.ihk-muenchen.de/de/Service/Digitalisierung/K%C3%BCnstliche-Intelligenz/AI-Act/ [7.10.2025]

Institut Zukunft des Lebens, 2025, Überblick über alle nationalen Umsetzungspläne des AI-Gesetzes (letzte Aktualisierung 19. Mai 2025), https://artificialintelligenceact.eu/de/national-implementation-plans/ [7.10.2025]

ISMS.online, 2024, The State of Information Security Report 2024, https://email.isms.online/hubfs/Brochures%2c%20guides%20and%20White%20Papers/Main%20Brochures/The%20State%20of%20Information%20Security%20Report%202024%20-%20ISMS.online%20V1.0.pdf [7.10.2025]

Joint Research Centre (JRC) / ENISA, 2024, Cyber Resilience Act Requirements Standards Mapping, https://www.enisa.europa.eu/sites/default/files/2024-11/Cyber%20Resilience%20Act%20Requirements%20Standards%20Mapping%20-%20final_with_identifiers_0.pdf [7.10.2025]

Joswig, Thomas / Kurz, Walter, 2025a, Empirical Analysis of NIS2 Adoption in EU SMEs: Challenges for Critical Infrastructure in Germany, Journal of Next-Generation Research 5.0, 1. Jg., Nr.3

Joswig, Thomas / Kurz, Walter, 2025b, Regulatory and Compliance Requirements for SMEs Operating AI Systems through Data Centers in the EU, with a Focus on Data Protection Challenges in Germany. Journal of Next-Generation Research 5.0., 1. Jg., Nr.2

Kajava, Kaisla / Gonzales Torres, Ana Paula / Rannisto, Antti / Sakai, Shintaro, 2025, Justifying AI regulation: Examining multi-stakeholder responses to the AI Act. Telematics and Informatics. 99. Jg., 102278, https://doi.org/10.1016/j.tele.2025.102278 [7.10.2025]

Kelber, Ulrich, 2025, Ohne Cybersicherheit kein Datenschutz. Gastbeitrag 23.05.2025 Handelsblatt live, https://live.handelsblatt.com/ohne-cybersicherheit-kein-datenschutz/ [7.10.2025]

Kikelj, Matija / Sabic, Ivan, 2024, Strengthening the Digital Ecosystem: Effects of the Cyber Resilience Act (CRA) on Open-Source Software. 2024 IEEE International Conference on Cyber Security and Resilience (CSR), S. 557–561

Laurer, Moritz / Renda, Andrea / Yeung, Timothy, 2021, Clarifying the costs for the EU's AI Act, https://www.ceps.eu/clarifying-the-costs-for-the-eus-ai-act/ [7.10.2025]

Mittelstand-Digital Zentrum Chemnitz (MDZ Chemnitz), 2025, Der EU AI-Act und was Unternehmen darüber wissen sollten, https://digitalzentrum-chemnitz.de/wissen/der-eu-ai-act-und-was-unternehmen-darueber-wissen-sollten/ [7.10.2025]

Mittelstand-Digital Zentrum Berlin (MDZ Berlin), 2025, Umsetzung des AI-Acts: Chancen skalieren, Risiken minimieren, https://digitalzentrum-berlin.de/veranstaltung/umsetzung-der-ki-verordnung-chancen-skalieren-risiken-minimieren [7.10.2025]

Mueck, Markus Dominik / Bar On, Amit Elazari / Du Boispean, Stephane, 2023, Upcoming European Regulations on Artificial Intelligence and Cybersecurity, IEEE Communications Magazine, 61. Jg., Nr. 7, S. 98–101

Mueller, Benjamin, 2021, How Much Will the Artificial Intelligence Act Cost Europe?, https://www2.datainnovation.org/2021-aia-costs.pdf [7.10.2025]

OpenKRITIS, 2024a, NIS2 Security Mapping, https://www.openkritis.de/massnahmen/nis2-mapping-standards-implementing.html [28.8.2025]

OpenKRITIS, 2024b, Critical Infrastructures and KRITIS in Germany, https://www.openkritis.de/eu/eu-nis-2-germany.html [7.10.2025]

Ramboll, 2024, Zwischenbericht: Begleitende und Ex-post-Evaluation des Förderschwerpunkts Mittelstand-Digital, im Auftrag des Bundesministeriums für Wirtschaft und Klimaschutz, https://www.bundeswirtschaftsministerium.de/Redaktion/DE/Publikationen/Digitale-Welt/3-zwischenbericht-mittelstand-digital-zentren.pdf?__blob=publicationFile&v=4 [7.10.2025]

Rane, Nitin / Choudary, Saurabh / Rane, Jayesh, 2024, Acceptance of artificial intelligence: key factors, challenges, and implementation strategies. SSRN Electronic Journal, https://doi.org/10.2139/ssrn.4842167 [7.10.2025]

Rat der Europäischen Union, 2020, Schlussfolgerungen des Rates zu Reallaboren und Experimentierklauseln als Instrumente für einen innovationsfreundlichen, zukunftssicheren und resilienten Rechtsrahmen zur Bewältigung disruptiver Herausforderungen im digitalen Zeitalter, https://data.consilium.europa.eu/doc/document/ST-13026-2020-INIT/de/pdf [7.10.2025]

Sánchez-Holgado, Patricia / Arcila-Calderón, Carlos, 2024, Adoption and use factors of artificial intelligence and big data by citizens. Communication & Society, https://doi.org/10.15581/003.37.2.227-246 [7.10.2025]

SANS / GIAC, 2025, 2025 Cybersecurity Workforce Research Report, https://www.sans.org/mlp/2025-attract-hire-retain-cybersecurity-roles [7.10.2025]

Sarra, Claudio, 2025, Artificial Intelligence in Decision-making: A Test of Consistency between the "EU AI Act" and the "General Data Protection Regulation", Athens Journal of Law, 11. Jg., Nr. 1, S. 45–62

SAS, 2024, forsa-Umfrage: Deutsche fühlen sich unwohl, wenn KI Entscheidungen trifft, https://www.sas.com/de_at/news/press-releases/2024/may/forsa-umfrage-deutsche-fuehlen-sich-unwohl-wenn-ki-entscheidungen-trifft.html [7.10.2025]

Scheufen, Marc, 2024a, Hemmnisse beim Data Sharing – Entwicklung und Handlungsempfehlungen, in: IW-Trends, 51. Jg., Nr. 2, S. 65–80

Scheufen, Marc, 2024b, Rechtliche Hemmnisse beim Data Sharing überwinden, IW-Kurzbericht, Nr. 31, Köln

Scheufen, Marc / Engels, Barbara / Schmitz, Edgar, 2025, Ziele, Nutzen-Kosten-Verhältnis und Hemmnisse Künstlicher Intelligenz in der deutschen Wirtschaft, in: IW-Trends, 52. Jg., Nr. 2, S. 67–86

SMEunited, 2022, Position paper on the initiative for a Cyber Resilience Act, https://www.smeunited.eu/admin/storage/smeunited/cyber-resilience-act-pp.pdf [7.10.2025]

Statistisches Bundesamt, 2025, Unternehmen (EU) (Unternehmensregister-System): Deutschland, Jahre, Wirtschaftszweige, Beschäftigtengrößenklassen, Genesis 52111

Tamó-Larrieux, Aurelia / Guitton, Clement / Mayer, Simon / Lutz, Christoph, 2023, Regulating for trust: Can law establish trust in artificial intelligence? Regulation & Governance, 18. Jg., S. 780–801

TÜV, 2025, Cybersicherheit in deutschen Unternehmen, https://www.tuev-verband.de/fileadmin/user_upload/Content_local/Studien_local/2025_TUEV-Verband_Cybersecurity-Studie_Studienbericht.pdf [7.10.2025]

TÜV AI.Lab, 2025, AI Act Risk Navigator, https://www.tuev-risk-navigator.ai/?lang=de [7.10.2025]

Winau, Mona, 2023, Areas of Tension in the Application of AI and Data Protection Law. European Data Protection Law Review, Jg. 9, Nr. 2/2023, S. 123–135, https://doi.org/10.21552/edpl/2023/2/7 [7.10.2025]

WEF – World Economic Forum, 2025, Global Cybersecurity Outlook 2025, https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf [7.10.2025]

ZUKIPRO, 2025, Zukunftszentrum für menschzentrierte KI in der Produktionsarbeit, https://www.zukipro.de/ [30.10.2025]