Praxisleitfaden zur NIS2-Compliance

Ein umfassender Leitfaden für kleine und mittlere Unternehmen zur Umsetzung der NIS2-Richtlinie der Europäischen Union

Welche Relevanz hat NIS2 für KMU?

Die NIS2-Richtlinie der EU bedeutet einen Paradigmenwechsel in der Regulierung der Cybersicherheit und betrifft erstmals zahlreiche kleine und mittlere Unternehmen (KMU) direkt. Während Cybersicherheit früher vorwiegend als Thema für Großunternehmen oder kritische Infrastrukturen galt, sind nun auch viele KMU dazu verpflichtet, ihre IT-Sicherheitsmaßnahmen deutlich zu professionalisieren. Die Gründe sind klar: Cyberangriffe nehmen zu, werden immer komplexer und können für KMU existenzbedrohend sein. Laut einer EU-Umfrage aus dem Jahr 2022 waren bereits 28 Prozent der KMU von Cyberkriminalität betroffen. NIS2 bietet jedoch auch die Chance, durch höhere Sicherheitsstandards Ausfallzeiten zu vermeiden und das Vertrauen von Kunden und Partnern zu stärken.

Vor diesem Hintergrund hat die Europäische Union im Jahr 2023 die NIS2-Richtlinie eingeführt, um den Schutz wichtiger Infrastrukturen vor IT-Störungen und Cyberangriffen zu stärken. Ihr Kernziel ist es, bestehende Sicherheitslücken zu schließen und eine einheitliche, höhere Sicherheitsgrundlage für alle Mitgliedstaaten zu schaffen, wodurch die allgemeine Cyberresilienz im öffentlichen und privaten Sektor verbessert wird.

Hinweis: Die NIS2-Richtlinie hätte bis zum 17. Oktober 2024 in nationales Recht umgesetzt werden müssen. Aufgrund der vorgezogenen Wahlen konnte das parlamentarische Verfahren zum NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG) jedoch nicht abgeschlossen werden.

NIS2-Timeline Deutschland

Q4 2025

Verabschiedung im Bundestag erwartet

Q1 2026

Inkrafttreten des Gesetzes

Q2 2026

Registrierungsphase für betroffene Unternehmen

Es wird geschätzt, dass die NIS2-Richtlinie in Deutschland etwa **30.000 Unternehmen** betreffen wird. Diese Unternehmen sind verpflichtet, geeignete IT-Sicherheitsmaßnahmen umzusetzen und erhebliche Sicherheitsvorfälle unverzüglich zu melden. Die EU-Richtlinie ist am 16. Januar 2023 in Kraft getreten und ersetzt die bisherige NIS1-Richtlinie mit Wirkung zum 18. Oktober 2024. Die nationale Umsetzung in Deutschland erfolgt durch das NIS2-Umsetzungsgesetz (NIS2UmsuCG), das sich derzeit (Stand: Juni 2025) noch im Gesetzgebungsverfahren befindet.

Persönliche Haftung der Geschäftsführung

Die Verantwortung für die Umsetzung der NIS2-Anforderungen liegt bei der Geschäftsführung des Unternehmens, die bei Verstößen **persönlich haftbar** gemacht werden kann und mit hohen Geldstrafen rechnen muss. Diese persönliche Haftung unterstreicht die Dringlichkeit des Engagements der Unternehmensleitung.

Das Abwarten bis zur endgültigen Verabschiedung des nationalen Gesetzes birgt ein hohes Risiko. Die Einhaltung der Richtlinie wird voraussichtlich unmittelbar nach Inkrafttreten des nationalen Gesetzes erwartet. Für KMU ist es von entscheidender Bedeutung, nicht nur Bußgelder zu vermeiden, sondern auch die Geschäftskontinuität und Wettbewerbsvorteile zu gewährleisten. Eine proaktive Umsetzung signalisiert den Partnern und Kunden gegenüber Zuverlässigkeit und kann potenziell neue Geschäfte anziehen, insbesondere da die Lieferkettensicherheit eine NIS2-Anforderung ist.

Was ist die NIS2-Richtlinie?

Die NIS2-Richtlinie, deren Abkürzung für "Network and Information Security" (Netz- und Informationssicherheit) steht, stellt die überarbeitete und erweiterte Version der ursprünglichen NIS-Richtlinie (NIS1) dar. Letztere ist offiziell als "Richtlinie (EU) 2022/2555" bezeichnet.

Das Ziel der NIS2-Richtlinie besteht darin, ein einheitlich hohes Schutzniveau für Netz- und Informationssysteme in 18 kritischen Sektoren zu etablieren. Die Richtlinie verpflichtet die Mitgliedstaaten, nationale Cybersicherheitsstrategien zu etablieren und die Zusammenarbeit bei der Reaktion auf Cybervorfälle zu intensivieren. Im Fokus stehen dabei der Schutz vor Cyberbedrohungen, die Sicherstellung der Geschäftskontinuität und die Minimierung von Risiken entlang der gesamten Lieferkette durch verpflichtende Sicherheitsanforderungen, verbindliche Risikomanagementmaßnahmen und eine schnelle Reaktion auf Sicherheitsvorfälle.

NIS2 stellt einen zentralen Bestandteil der umfassenden Cybersicherheitsstrategie der EU dar. Sie legt einen Mindeststandard fest, der es den einzelnen Mitgliedstaaten ermöglicht, strengere Vorschriften zu erlassen. Die Richtlinie verpflichtet die Mitgliedstaaten, nationale Cybersicherheitsstrategien zu verabschieden, zuständige nationale Behörden (wie das BSI in Deutschland) zu benennen, Behörden für das Cyberkrisenmanagement (CyCLONe) und Computer-Notfallteams (CSIRTs) einzurichten.

Aktuelle Entwicklung

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) wird laut aktuellem Gesetzesentwurf deutlich mehr Kompetenzen erhalten und als zentrale Anlaufstelle für die Umsetzung der NIS2-Richtlinie in Deutschland fungieren. Die personellen Kapazitäten des BSI sollen dafür erheblich aufgestockt werden.

Verhältnis zur DSGVO

Die NIS2-Richtlinie steht in engem Zusammenhang mit der DSGVO. Beide verfolgen das Ziel, die Sicherheit und den Schutz personenbezogener Daten zu gewährleisten. Sicherheitsvorfälle sind sowohl nach NIS2 als auch nach der DSGVO zu melden.

NIS vs. NIS2: Wesentliche Neuerungen

Im Vergleich zur Vorgängerrichtlinie bringt NIS2 erhebliche Erweiterungen mit sich:

Erweiterter Anwendungsbereich

Deutlich mehr betroffene Sektoren

Strengere Anforderungen

Höhere Sicherheitsstandards für Unternehmen

Harmonisierte Sanktionen

Einheitlicher Rahmen in allen EU-Mitgliedstaaten

Verschärfte Meldepflichten

Kürzere Fristen bei Sicherheitsvorfällen

Lieferkettenfokus

Stärkere Betonung der Lieferkettensicherheit

Aspekt	NIS-Richtlinie	NIS2-Richtlinie
Sektoren	Wenige kritische Infrastrukturen (z.B. Energie, Transport, Banken, Gesundheitswesen)	18 Sektoren inkl. digitale Infrastrukturen, öffentliche Verwaltung, Raumfahrt, Abfallwirtschaft, Lebensmittelproduktion
Größenkriterien	Große Unternehmen	Große und mittelgroße Unternehmen (über 50 Mitarbeiter oder über 10 Mio. Euro Umsatz)
Sanktionen	Bußgelder bis zu 1 Mio. Euro oder 2 % des Jahresumsatzes	Bis 10 Mio. € oder 2 % Umsatz (wesentliche Einrichtungen); bis 7 Mio. € oder 1,4 % Umsatz (wichtige Einrichtungen)
Management-Haftung	Nicht vorgesehen	Persönliche Haftung und direkte Verantwortung der Geschäftsleitung
Meldepflichten	Meldung von Vorfällen ohne feste Fristen	Erstmeldung innerhalb von 24 Stunden, Detailbericht nach 72 Stunden, Abschlussbericht nach spätestens einem Monat
Sicherheitsanforderungen	Grundlegende Sicherheitsmaßnahmen, keine einheitlichen Mindeststandards	Verbindliche Mindeststandards, Risikomanagement, regelmäßige Überprüfungen, Mehrfaktorauthentifizierung, Lieferantenkontrollen

Betroffene Unternehmen

In der NIS2-Richtlinie werden "wesentliche" und "wichtige" Einrichtungen in 18 verschiedenen Sektoren unterschieden. Beide Kategorien unterliegen regulatorischen Anforderungen, deren Intensität jedoch unterschiedlich ist.

Sektor	Beispiele für betroffene Unternehmen	Kategorie
Energie	Stromversorger, Gasnetzbetreiber, Mineralölunternehmen	Wesentlich
Verkehr	Flughäfen, Bahnunternehmen, Reedereien, Logistikunternehmen	Wesentlich
Bankwesen	Kreditinstitute, Zahlungsdienstleister	Wesentlich
Gesundheitswesen	Krankenhäuser, Labore, Pharmaunternehmen	Wesentlich
Digitale Infrastruktur	Rechenzentren, Cloud-Anbieter, DNS-Dienstleister	Wesentlich
Öffentliche Verwaltung	Bundesbehörden, Landesbehörden, Kommunen	Wesentlich
Digitale Dienstleister	Online-Marktplätze, Suchmaschinen, Social-Media Plattformen	Wichtig
Postdienste	Postdienstleister, Kurierdienste	Wichtig
Abfallwirtschaft	Entsorgungsunternehmen	Wichtig
Herstellung	Hersteller kritischer Produkte (z.B. Medizinprodukte)	Wichtig

Größenkriterien

Ein zentrales Kriterium für die Anwendbarkeit der NIS2-Richtlinie ist die Unternehmensgröße. Grundsätzlich fallen alle mittleren und großen Unternehmen in den genannten Sektoren unter die Richtlinie:

Wesentliche Einrichtungen

Unternehmen mit mindestens **250 Mitarbeitenden** oder einem Jahresumsatz von mindestens **50 Millionen Euro** und einer Jahresbilanzsumme von über **43 Millionen Euro**

Wichtige Einrichtungen

Unternehmen mit mindestens **50 Mitarbeitenden** oder einem Jahresumsatz von mehr als **10 Millionen Euro** und einer Bilanzsumme von mehr als **10 Millionen Euro**

Sonderfälle: Unabhängig von der Größe sind auch bestimmte Betreiber wie qualifizierte Vertrauensdienste, TLD-Registries, DNS-Dienste und manche öffentliche Stellen immer erfasst. Kleinere Unternehmen können ebenfalls betroffen sein, wenn sie eine besondere Bedeutung für ihre Region oder Lieferkette haben.

Wichtig

Auch wenn Ihr Unternehmen nicht direkt unter die NIS2-Richtlinie fällt, können Sie indirekt betroffen sein, wenn Sie als Zulieferer oder Dienstleister für regulierte Unternehmen tätig sind. Diese werden zunehmend Nachweise über Ihre Cybersicherheitsmaßnahmen verlangen. Unternehmen in der Lieferkette müssen daher ebenfalls mit neuen Anforderungen rechnen.

Sanktionen und Bußgelder nach NIS2

Die NIS2-Richtlinie bringt deutlich verschärfte Sanktionen für Unternehmen und Einrichtungen, die die Anforderungen an die Cybersicherheit nicht erfüllen. Die Höhe der Bußgelder richtet sich dabei nach der Einstufung der betroffenen Organisation als "wesentliche Einrichtung" oder "wichtige Einrichtung".

Kategorie	Max. Bußgeld (absolut)	Max. Bußgeld (relativ)	Maßgeblich ist der höhere Betrag
Wesentliche Einrichtungen	**10 Mio. Euro**	**2 % des weltweiten Jahresumsatzes**	Ja
Wichtige Einrichtungen	**7 Mio. Euro**	**1,4% des weltweiten Jahresumsatzes**	Ja

Die Sanktionen werden gemäß § 65 BSIG (Entwurf) verhängt und orientieren sich an der Schwere des Verstoßes sowie der Größe und Bedeutung der Einrichtung.

Anwendungsbeispiele für Verstöße

- Nichtumsetzung oder unvollständige Umsetzung von Cybersicherheitsmaßnahmen
- Nicht- oder verspätete Meldung von Sicherheitsvorfällen
- Verletzung von Melde- und Dokumentationspflichten
- Missachtung von Anweisungen der Aufsichtsbehörden

Weitere Sanktionsmöglichkeiten

Persönliche Haftung

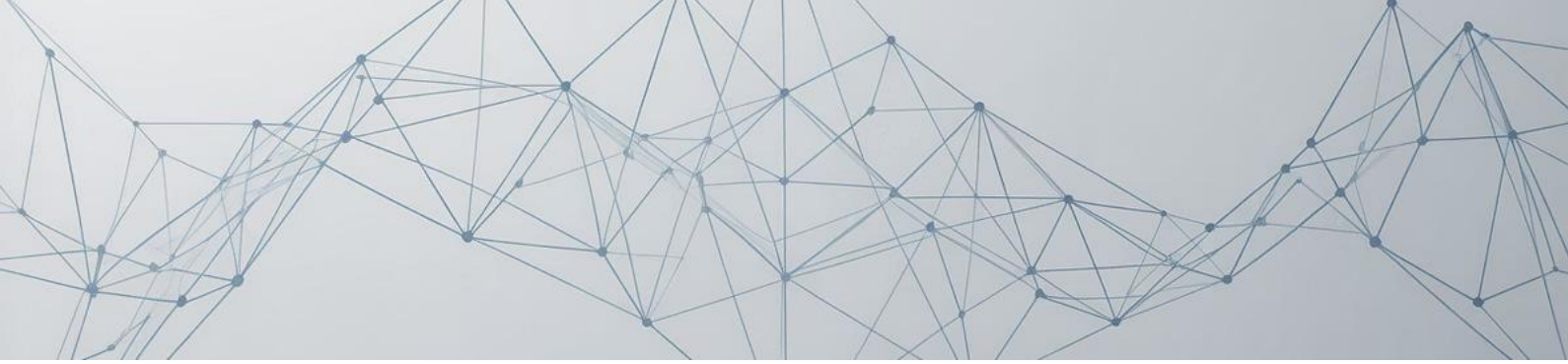
Die Geschäftsverantwortlichen können im Rahmen der Binnenhaftung zur Verantwortung gezogen werden, wenn sie ihren Pflichten zur Überwachung und Umsetzung der Cybersicherheitsmaßnahmen nicht nachkommen.

Audits und Überprüfungen

Nationale Aufsichtsbehörden können regelmäßige Audits durchführen und bei Verstößen die oben genannten Sanktionen verhängen.

Bemessung und Durchsetzung

- Maßgeblich ist jeweils der höhere Betrag zwischen absolutem Höchstbetrag und dem prozentualen Anteil am weltweiten Jahresumsatz.
- Die Durchsetzbarkeit der Bußgelder wird als ähnlich wie bei der DSGVO eingeschätzt, d. h. die tatsächliche Verhängung hängt von der Kapazität und Aktivität der zuständigen Behörden ab.



Umfang der Pflichten für KMU: Was NIS2 von Ihnen fordert

Die NIS2-Richtlinie legt eine Reihe konkreter Pflichten fest, die betroffene KMU umsetzen müssen, um ihre Cybersicherheit zu stärken und die Resilienz gegenüber Cyberbedrohungen zu erhöhen.

1 Risikomanagement

Systematische Erfassung und Bewertung potenzieller Bedrohungen und Schwachstellen, dokumentierte Risikoanalyse, regelmäßige Sicherheitsbewertungen.

2 ISMS

Einführung eines Informationssicherheitsmanagementsystems nach ISO 27001 oder BSI IT-Grundschutz zur strukturierten Umsetzung.

3 Meldepflichten

Vorfälle mit erheblicher Auswirkung müssen innerhalb von 24 Stunden vorläufig und binnen 72 Stunden vollständig an das BSI gemeldet werden.

4 Lieferkette

Prüfung von Dienstleistern und Partnern auf angemessene Sicherheitsstandards. Vertragsregelungen und regelmäßige Audits empfohlen.

5 Schulungen

Regelmäßige, zielgruppengerechte Awareness-Trainings zu Themen wie Phishing, Passwortschutz und IT-Hygiene.

6 BCM

Entwicklung und Test eines Notfall- und Wiederherstellungsplans für den Fall eines IT-Ausfalls (Business Continuity Management).

Geschäftsführungsverantwortung

Die Verantwortung für die Umsetzung liegt bei der Geschäftsführung. Sie ist verpflichtet, ihre eigene Cyberkompetenz zu stärken und haftet im Zweifelsfall persönlich für Verstöße gegen die Vorgaben der Richtlinie.

Herausforderungen für KMU bei der Umsetzung von NIS2

Die Umsetzung der NIS2-Richtlinie stellt KMU vor spezifische Herausforderungen, bietet aber gleichzeitig erhebliche Chancen.

! Herausforderungen

- Beträchtlicher Ressourcenaufwand für spezialisiertes Personal und IT-Budgets
- Komplexe Anforderungen an Dokumentation und Risikobewertung
- Zeitlicher Druck ohne Übergangsfrist
- Fehlende Erfahrung mit regulatorischen Sicherheitsvorgaben

+ Chancen

- Strategischer Wettbewerbsvorteil durch nachweislich hohe Sicherheitsstandards
- Stärkung des Vertrauens von Kunden, Partnern und Investoren
- Entscheidender Faktor in Lieferbeziehungen
- Kostenreduzierung durch weniger IT-Ausfälle

Für eine Vielzahl von KMU kann es von Vorteil sein, auf externe Expertise, wie SecuraTrust, zurückzugreifen. Die Umsetzung wird von uns in strukturierter Form begleitet, es werden Schulungen durchgeführt und bei der Einführung eines ISMS wird Hilfestellung geleistet. Diese Option trägt zur Reduzierung der internen Komplexität bei und ermöglicht eine wirtschaftlich skalierbare Compliance.

Handlungsempfehlungen für KMU

Um den Anforderungen der NIS2-Richtlinie gerecht zu werden, empfehlen wir Unternehmen ein systematisches und proaktives Vorgehen. Folgende Schritte sind essenziell:

1. Betroffenheitsanalyse

Prüfen Sie, ob Ihr Unternehmen unter die NIS2-Richtlinie fällt und in welche Kategorie (wesentlich oder wichtig) es einzuordnen ist. Berücksichtigen Sie dabei auch Sonderfälle und aktuelle Schwellenwerte.

2. Gap-Analyse

Ermitteln Sie den Abstand zwischen Ihrem aktuellen Sicherheitsniveau und den Anforderungen der NIS2-Richtlinie. Nutzen Sie dazu Checklisten oder externe Beratung, um alle relevanten Aspekte abzudecken.

3. Governance-Strukturen

Etablieren Sie klare Verantwortlichkeiten für Cybersicherheit auf Leitungsebene. Schulen Sie Geschäftsleitung und Führungskräfte regelmäßig zu ihren Pflichten – die NIS2 sieht explizit eine Managementhaftung vor.

4. Risikomanagement

Implementieren Sie ein systematisches Risikomanagement für Cybersicherheit, das regelmäßige Bewertungen, die Berücksichtigung neuer Bedrohungen und die Anpassung von Schutzmaßnahmen umfasst.

5. Incident Response

Entwickeln Sie einen Prozess zur Erkennung, Meldung und Bewältigung von Sicherheitsvorfällen. Beachten Sie die verschärften Meldefristen: Erstmeldung innerhalb von 24 Stunden, Detailbericht nach 72 Stunden, Abschlussbericht spätestens nach einem Monat.

6. Lieferkettensicherheit

Überprüfen Sie Ihre Lieferanten und Dienstleister auf Cybersicherheitsrisiken und integrieren Sie entsprechende Anforderungen und Nachweispflichten in Ihre Verträge. Dokumentieren Sie die Überprüfung regelmäßig.

7. Sensibilisierung & Schulung

Schulen und sensibilisieren Sie alle Beschäftigten regelmäßig für Cybersicherheitsrisiken und Meldewege. Fördern Sie eine Sicherheitskultur im Unternehmen.

8. Kontinuierliche Überprüfung

Überprüfen und aktualisieren Sie Ihre Sicherheitsmaßnahmen, Prozesse und Richtlinien regelmäßig – mindestens jährlich oder bei wesentlichen Änderungen.

Besonders wichtig ist ein strukturierter Ansatz. Viele Unternehmen entscheiden sich für die Implementierung eines Informationssicherheits-Managementsystems (ISMS) nach ISO 27001 oder BSI IT-Grundschutz, da dies viele der NIS2-Anforderungen abdeckt und einen anerkannten Rahmen für Cybersicherheit bietet.

Praxistipp

Beginnen Sie mit einer Inventarisierung Ihrer kritischen Systeme, Prozesse und Daten. Dies bildet die Grundlage für alle weiteren Maßnahmen und hilft Ihnen, Ihre Ressourcen gezielt auf die wichtigsten Bereiche zu konzentrieren.

Ausblick: Zukünftige Entwicklungen

Weitere wichtige EU-Gesetzgebungsakte

Cybersicherheits-Regulierung

DORA - Digital Operational Resilience Act

Die Regelung findet unmittelbar Anwendung auf Unternehmen der Finanzbranche (beispielsweise Banken, Versicherungen und Zahlungsdienstleister) und stellt strenge Anforderungen an deren digitale operationelle Resilienz, insbesondere in den Bereichen IKT-Risiko, Vorfallmanagement und Drittparteimanagement.

Stand: Die Regelung ist seit Januar 2025 in Kraft und derzeit befinden sich zahlreiche Unternehmen in der aktiven Implementierungsphase.

CRA - Cyber Resilience Act

Erstmalige Festlegung gemeinsamer Cybersicherheitsstandards für Produkte mit digitalen Elementen (beispielsweise IoT-Geräte, Software) auf EU-weiter Ebene sowie die Einführung von Sorgfalts- und Meldepflichten für Hersteller, Importeure und Händler.

Stand: Im Frühjahr 2025 verabschiedet, ist die verpflichtende Anwendung ab 2027 zu erwarten.

Notfall- und Krisenmanagement

CSA - Cyber Solidarity Act

Zielt auf die Verbesserung der Abwehrbereitschaft, Prävention und Reaktion auf größere Cybersicherheitsvorfälle in der gesamten Europäischen Union ab. Schafft unter anderem ein europäisches Cyber-Notfallteam-Netzwerk (Cybersecurity Emergency Response Teams, CyCLONe).

Stand: Verabschiedet im Mai 2025, derzeit erfolgt die EU-weite Etablierung erster Maßnahmen und Strukturen.

CER-Richtlinie (Critical Entities Resilience Directive)

Ergänzt NIS2 und stärkt die physische und organisatorische Resilienz kritischer Infrastrukturen gegen eine Vielzahl von Bedrohungen, einschließlich Cyberangriffen, Naturkatastrophen und Sabotage.

Stand: Die Regelung ist seit Oktober 2024 in Kraft getreten, nationale Umsetzung läuft; erste Maßnahmen werden in den Mitgliedstaaten eingeführt.

Datenschutz und Awareness

DSGVO (Datenschutz-Grundverordnung)

Die DSGVO schützt personenbezogene und insbesondere sensible Daten durch hohe Anforderungen an die Datensicherheit und verpflichtet Unternehmen zur Umsetzung geeigneter Schutzmaßnahmen.

Stand: Die Regelung ist seit Mai 2018 in Kraft und hat eine übliche Anpassung der Prozesse in den meisten Unternehmen zur Folge. Es finden regelmäßige Überprüfungen statt.

ECSM - EU Cybersecurity Month

Im Oktober findet jährlich eine Kampagne statt, die europaweit durchgeführt wird. Diese dient dazu, die Sicherheit im Bereich des Cyberspace zu fördern, die Öffentlichkeit zu sensibilisieren und die digitale Kompetenz zu stärken.

Stand: Seit dem Jahr 2012 etabliert und seither jährlich durchgeführt, wobei eine stetige Weiterentwicklung der Inhalte und Reichweite zu verzeichnen ist.

Fazit für Unternehmen

Die NIS2-Richtlinie und die genannten ergänzenden Regelwerke demonstrieren, dass die EU eine umfassende und dynamische Strategie für Cybersicherheit verfolgt. Unternehmen sind gefordert, sich kontinuierlich an neue Bedrohungen und regulatorische Anforderungen anzupassen. Die Integration von Cybersicherheit und Datenschutz in die Unternehmensstrategie wird von entscheidender Bedeutung sein, um in dieser sich entwickelnden Landschaft Resilienz und Wettbewerbsfähigkeit zu gewährleisten.

Torsten Drews

Executive Advisor | Experte für IT-Compliance, Informationssicherheit und Governance in KMU.

Jetzt Kontakt aufnehmen

Erstellt am: 02.06.2025 | Bearbeitet am: 23.10.2025