



## IT-SiG 2.0, EU NIS 2 und EU RCE Erhöhung der Resilienz im Kontext der Cybersicherheit

### Wachsende Pflichten und Herausforderungen

Unternehmen sämtlicher Branchen geraten zunehmend in den Fokus von Cyberangriffen. Die Gesetzgebung begegnet diesen Herausforderungen durch Regulierungen auf nationaler und europäischer Ebene: Neben dem bestehenden deutschen IT-Sicherheitsgesetz 2.0 wurden auf europäischer Ebene die EU NIS 2 Directive sowie EU RCE verabschiedet, die bis spätestens Oktober 2024 in die nationale Gesetzgebung überführt werden sollen. In diesem Kontext liegen bereits Referententwürfe des NIS 2-Umsetzungsgesetzes (NIS 2 UmsuCG) sowie des KRITIS-Dachgesetzes (KRITIS-DachG) vor.

### Konsequenz für bisher nicht regulierte Unternehmen

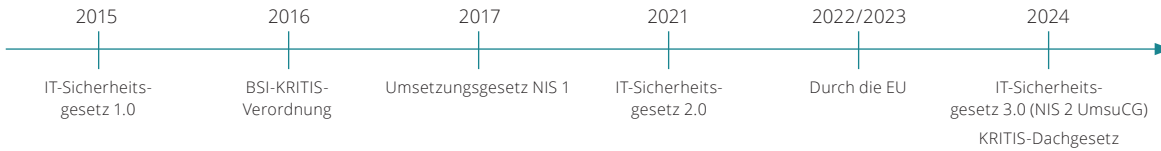
Eine Vielzahl von Unternehmen wird zukünftig gemäß EU NIS 2 sowie EU RCE verpflichtet und haftbar gemacht, Mindestanforderungen an Cybersicherheit und Resilienz einzuhalten. Die Zahl der regulierten Unternehmen wird stark ansteigen.

### Konsequenz für Betreiber kritischer Infrastrukturen nach IT-SiG 2.0

Betreiber kritischer Infrastrukturen sind in besonderem Maße Ziel von Angriffen und werden zukünftig noch stärker reguliert – die Anforderungen steigen. ➔

## Was kommt auf Ihr Unternehmen zu?

Abb. 1 – Entwicklung des IT-Sicherheitsrechts



### EU NIS 2 Cybersecurity

Die EU NIS 2 Directive legt erweiterte Anforderungen für Betreiber kritischer Infrastrukturen fest. Unternehmen mit mindestens 50 Mitarbeitern oder einem Umsatz von 10 Millionen Euro, die in einem von 18 NIS 2-Sektoren tätig sind, fallen nun hierunter. Sicherheitsanforderungen werden verstärkt und umfassen Lieferketten, wobei die entsprechenden Sanktionen erhöht wurden. In Deutschland wird das NIS 2-Umsetzungsgesetz diese EU-Richtlinien ab 2024 in das nationale Recht überführen. Dies wird voraussichtlich rund 30.000 Unternehmen betreffen, u.a. Betreiber kritischer Infrastrukturen nach dem IT-SiG 2.0.

### EU RCE – CER-Richtlinie

Die kürzlich verabschiedete CER-Richtlinie (EU 2022/2557), auch bekannt als EU RCE Directive, zielt auf die Stärkung der Resilienz kritischer Infrastrukturen in der EU ab.

Die Richtlinie schreibt Mindestmaßnahmen zur Absicherung der Resilienz vor, inklusive Vorsorge, physischer Sicherheit, Krisenmanagement und Awareness-Maßnahmen. Wesentliche Störungen und Vorfälle müssen den nationalen Behörden innerhalb von 24 Stunden gemeldet werden.

Unternehmen, die in sechs oder mehr EU-Staaten tätig sind, müssen sich einer zusätzlichen Überprüfung unterziehen. Zudem setzt das KRITIS-Dachgesetz, das ab 2024 in Deutschland in Kraft tritt, weitere Pflichten fest, einschließlich Meldepflichten und Geschäftskontinuitätsmanagement (BCM).

### Wie wir Sie unterstützen können

Unser Ziel ist es, jegliche Unternehmen und Organisationen dabei zu unterstützen, einen hohen Sicherheitsstandard zu erreichen und den diversen Regulierungen und Risiken entgegenzutreten. Dafür haben wir folgendes Portfolio entwickelt:

IT-Sicherheitsberatung und -Assurance	Risikomanagement-Beratung und -Assurance	Physische Sicherheitsberatung und -Assurance	Betrachtung der Systeme zur Angriffserkennung
<ul style="list-style-type: none"> <li>• Unterstützung beim Aufbau von Informationssicherheitsmanagementsystemen (ISMS)</li> <li>• Betroffenheitsanalysen KRITIS, EU NIS 2 und EU RCE</li> <li>• Durchführung von Readiness Assessments zur Erfüllung aktueller regulatorischer Anforderungen</li> <li>• Analyse und Beurteilung von Notfall- und Krisenmanagementstrukturen, -prozessen und -maßnahmen</li> <li>• Durchführung von Awareness-Kampagnen und -Workshops zu aktuellen IT-Sicherheitsaspekten und regulatorischen Anforderungen</li> </ul>	<ul style="list-style-type: none"> <li>• Unterstützung bei der strukturierten Identifizierung potenzieller Risiken und Entwicklung von Risikobehandlungsoptionen</li> <li>• Überprüfung Ihres bestehenden Risikomanagements inkl. Reportingstrukturen und Verantwortlichkeiten nach ausgewählten Normen und/oder regulatorischen Anforderungen</li> <li>• Identifikation und Implementierung von Sicherheitsmaßnahmen inkl. Risikoanalyse nach IT-Grundschutz</li> </ul>	<ul style="list-style-type: none"> <li>• Überprüfung der Sicherheit von Gebäuden, Anlagen und Ausrüstung; Identifikation von Schwachstellen und deren Behebung</li> <li>• Ist-Aufnahme bestehender baulicher, technischer und organisatorischer Maßnahmen, Soll-Konzeptentwicklung und Roadmap-Erstellung zur Erreichung des gewünschten Sicherheitsniveaus</li> <li>• Unterstützung bei der Ausarbeitung von Notfallszenarien sowie der Planung und Durchführung von Notfalltests und -übungen</li> </ul>	<ul style="list-style-type: none"> <li>• Unterstützung bei der Erstellung wirksamer Angriffserkennungsstrategien</li> <li>• Identifizierung potenzieller Bedrohungsvektoren und Entwicklung von Reaktionsrichtlinien</li> <li>• Überprüfung vorhandener Sicherheitskonzepte auf Effektivität; Überprüfung der vollständigen Einbindung von Informationsquellen und der ausgewerteten Ereignisse auf Angemessenheit</li> <li>• Durchführung von Workshops zu aktuellen regulatorischen Anforderungen (KRITIS) an Systeme zur Angriffserkennung</li> </ul>

Lassen Sie uns gemeinsam ein auf Ihre Anforderungen abgestimmtes Paket zusammenstellen und Ihre Herausforderungen lösen. Sprechen Sie uns gerne an unter [kritis@deloitte.de](mailto:kritis@deloitte.de).

## Kontakte



### **Oliver Migge**

Director

Tel: +49 151 5800 2160

[omigge@deloitte.de](mailto:omigge@deloitte.de)



### **Janika Schauer**

Manager

Tel: +49 151 5807 0371

[janschauer@deloitte.de](mailto:janschauer@deloitte.de)

# Deloitte.

Deloitte bezieht sich auf Deloitte Touche Tohmatsu Limited (DTTL), ihr weltweites Netzwerk von Mitgliedsunternehmen und ihre verbundenen Unternehmen (zusammen die „Deloitte-Organisation“). DTTL (auch „Deloitte Global“ genannt) und jedes ihrer Mitgliedsunternehmen sowie ihre verbundenen Unternehmen sind rechtlich selbstständige und unabhängige Unternehmen, die sich gegenüber Dritten nicht gegenseitig verpflichten oder binden können. DTTL, jedes DTTL-Mitgliedsunternehmen und verbundene Unternehmen haften nur für ihre eigenen Handlungen und Unterlassungen und nicht für die der anderen. DTTL erbringt selbst keine Leistungen gegenüber Mandanten. Weitere Informationen finden Sie unter [www.deloitte.com/de/UeberUns](http://www.deloitte.com/de/UeberUns).

Deloitte bietet branchenführende Leistungen in den Bereichen Audit und Assurance, Steuerberatung, Consulting, Financial Advisory und Risk Advisory für nahezu 90% der Fortune Global 500®-Unternehmen und Tausende von privaten Unternehmen an. Rechtsberatung wird in Deutschland von Deloitte Legal erbracht. Unsere Mitarbeitenden liefern messbare und langfristig wirkende Ergebnisse, die dazu beitragen, das öffentliche Vertrauen in die Kapitalmärkte zu stärken, die unsere Kunden bei Wandel und Wachstum unterstützen und den Weg zu einer stärkeren Wirtschaft, einer gerechteren Gesellschaft und einer nachhaltigen Welt weisen. Deloitte baut auf eine über 175-jährige Geschichte auf und ist in mehr als 150 Ländern tätig. Erfahren Sie mehr darüber, wie die rund 457.000 Mitarbeitenden von Deloitte das Leitbild „making an impact that matters“ täglich leben: [www.deloitte.com/de](http://www.deloitte.com/de).

Diese Veröffentlichung enthält ausschließlich allgemeine Informationen. Weder die Deloitte GmbH Wirtschaftsprüfungsgesellschaft noch Deloitte Touche Tohmatsu Limited („DTTL“), ihr weltweites Netzwerk von Mitgliedsunternehmen noch deren verbundene Unternehmen (zusammen die „Deloitte-Organisation“) erbringen mit dieser Veröffentlichung eine professionelle Dienstleistung. Diese Veröffentlichung ist nicht geeignet, um geschäftliche oder finanzielle Entscheidungen zu treffen oder Handlungen vorzunehmen. Hierzu sollten Sie sich von einem qualifizierten Berater in Bezug auf den Einzelfall beraten lassen.

Es werden keine (ausdrücklichen oder stillschweigenden) Aussagen, Garantien oder Zusicherungen hinsichtlich der Richtigkeit oder Vollständigkeit der Informationen in dieser Veröffentlichung gemacht, und weder DTTL noch ihre Mitgliedsunternehmen, verbundene Unternehmen, Mitarbeiter oder Bevollmächtigten haften oder sind verantwortlich für Verluste oder Schäden jeglicher Art, die direkt oder indirekt im Zusammenhang mit Personen entstehen, die sich auf diese Veröffentlichung verlassen. DTTL und jede ihrer Mitgliedsunternehmen sowie ihre verbundenen Unternehmen sind rechtlich selbstständige und unabhängige Unternehmen.