Deloitte.

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 Referentenentwürfe 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.

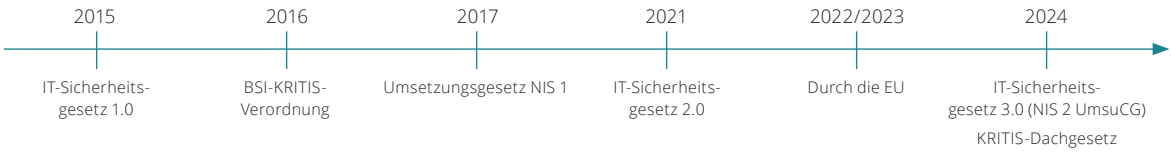
Konsequenz für Betreiber kritischer Infrastrukturen nach IT-SiG 2.0

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

MAKING AN IMPACT THAT MATTERS since 1845

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

- Unterstützung beim Aufbau von Informationssicherheits-managementsystemen (ISMS)
- Betroffenheitsanalysen KRITIS, EU NIS 2 und EU RCE
- Durchführung von Readiness Assessments zur Erfüllung aktueller regulatorischer Anforderungen
- Analyse und Beurteilung von Notfall- und Krisen-managementstrukturen, -prozessen und -maßnahmen
- Durchführung von Awareness-Kampagnen und -Workshops zu aktuellen IT-Sicherheitsaspekten und regulatorischen Anforderungen

Risikomanagement-Beratung und -Assurance

- Unterstützung bei der strukturierten Identifizierung potenzieller Risiken und Entwicklung von Risikobehandlungsoptionen
- Überprüfung Ihres bestehenden Risikomanagements inkl. Reportingstrukturen und Verantwortlichkeiten nach ausgewählten Normen und/oder regulatorischen Anforderungen
- Identifikation und Implementierung von Sicherheitsmaßnahmen inkl. Risikoanalyse nach IT-Grundschutz

Physische Sicherheitsberatung und -Assurance

- Überprüfung der Sicherheit von Gebäuden, Anlagen und Ausrüstung; Identifikation von Schwachstellen und deren Behebung
- Ist-Aufnahme bestehender baulicher, technischer und organisatorischer Maßnahmen, Soll-Konzeptentwicklung und Roadmap-Erstellung zur Erreichung des gewünschten Sicherheitsniveaus
- Unterstützung bei der Ausarbeitung von Notfallszenarien sowie der Planung und Durchführung von Notfalltests und -übungen

Betrachtung der Systeme zur Angriffserkennung

- Unterstützung bei der Erstellung wirksamer Angriffserkennungsstrategien
- Identifizierung potenzieller Bedrohungsvektoren und Entwicklung von Reaktionsrichtlinien
- Überprüfung vorhandener Sicherheitskonzepte auf Effektivität; Überprüfung der vollständigen Einbindung von Informationsquellen und der ausgewerteten Ereignisse auf Angemessenheit
- Durchführung von Workshops zu aktuellen regulatorischen Anforderungen (KRITIS) an Systeme zur Angriffserkennung

Lassen Sie uns gemeinsam ein auf Ihre Anforderungen abgestimmtes Paket zusammenstellen und Ihre Herausforderungen lösen. Sprechen Sie uns gerne an unter kritis@deloitte.de.

Kontakte

Oliver Migge
Director
Tel: +49 151 5800 2160
omigge@deloitte.de

Janika Schauer
Manager
Tel: +49 151 5807 0371
janschauer@deloitte.de

Deloitte.

Stand 3/2024