NOVATEC
DIE BESTEN IDEEN FÜR IHRE SICHERHEIT

EXECUTIVE WHITEPAPER

# KRITIS & NIS 2: Anforderungen, Risiken & Handlungsfelder

Regulatorische Anforderungen erfüllen.
Kritische Infrastrukturen schützen.

**Von Compliance zu Resilienz:**
Sicherheitsarchitektur im Wandel

Die zunehmende Digitalisierung kritischer Infrastrukturen sowie die steigende Komplexität von Bedrohungsszenarien führen dazu, dass regulatorische Anforderungen wie das KRITIS-Dachgesetz, die NIS2-Richtlinie und der Cyber Resilience Act erheblich an Bedeutung gewinnen. Sie definieren verbindliche Rahmenbedingungen für die Sicherheit und Resilienz von Organisationen, die essenzielle gesellschaftliche Funktionen bereitstellen.

Für Betreiber kritischer Infrastrukturen bedeutet dies nicht nur die Erfüllung regulatorischer Vorgaben, sondern vor allem die Notwendigkeit, bestehende Sicherheitsarchitekturen ganzheitlich weiterzuentwickeln.

Dieses Whitepaper gibt einen strukturierten Überblick über zentrale Anforderungen und zeigt auf, wie ein integrierter Sicherheitsansatz dazu beitragen kann, Risiken zu reduzieren, Ausfallzeiten zu minimieren und die langfristige Resilienz nachhaltig zu stärken.

# INHALT

# 01 Einleitung

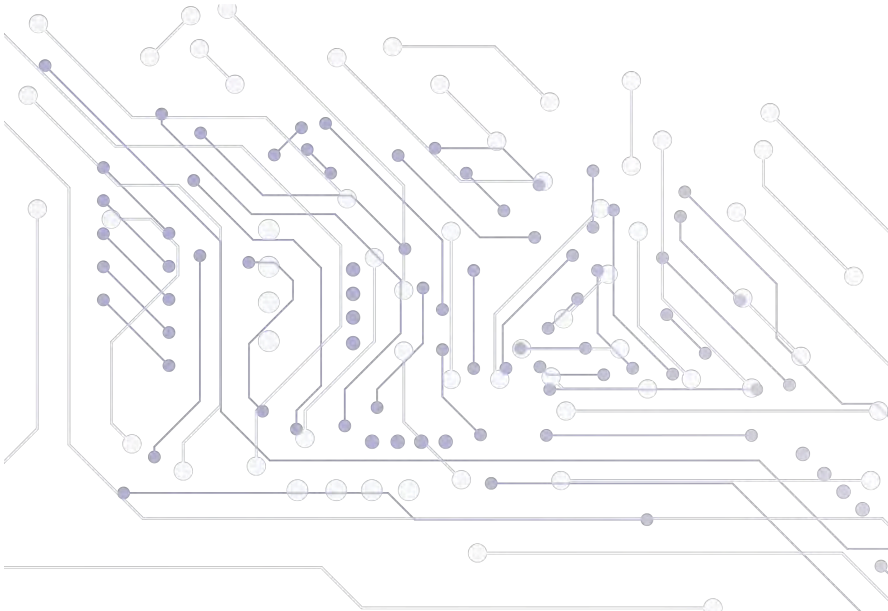
Die zunehmende Digitalisierung, Vernetzung und Automatisierung von Gebäuden, Anlagen und Prozessen schafft neue Effizienzpotenziale, erweitert jedoch zugleich die Angriffsfläche für Cyberangriffe, Sabotage und andere sicherheitsrelevante Vorfälle. Davon betroffen sind längst nicht mehr nur Betreiber kritischer Infrastrukturen. Auch Industrieunternehmen, öffentliche Einrichtungen und Organisationen aller Größenordnungen sehen sich wachsenden Anforderungen an die Resilienz ihrer physischen und digitalen Infrastruktur gegenüber.

Mit dem KRITIS-Dachgesetz und der Umsetzung der NIS-2-Richtlinie hat der Gesetzgeber den regulatorischen Rahmen deutlich verschärft. Sicherheit und Risikomanagement werden damit zunehmend zu strategischen Managementaufgaben und zu einem wesentlichen Bestandteil der Unternehmensführung.

Dieses Whitepaper bietet einen kompakten Überblick über die aktuellen gesetzlichen Anforderungen und deren praktische Auswirkungen. Es erläutert zentrale Begriffe und Pflichten, zeigt wirksame Maßnahmen zur Risikominimierung auf und beschreibt, wie ein ganzheitlicher Sicherheitsansatz dazu beitragen kann, regulatorische Vorgaben zu erfüllen und gleichzeitig die Widerstandsfähigkeit der eigenen Infrastruktur nachhaltig zu stärken.

Darüber hinaus erfahren Sie, welche organisatorischen, technischen und infrastrukturellen Maßnahmen jetzt relevant sind, um Compliance-Anforderungen zu erfüllen, Sicherheitsrisiken zu reduzieren und Ihre Organisation zukunftssicher aufzustellen.

Die in diesem Whitepaper enthaltenen Informationen beziehen sich auf das am 17. März 2026 in Kraft getretene KRITIS-Dachgesetz sowie auf das Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung, veröffentlicht am 5. Dezember 2025 und in Kraft getreten am 6. Dezember 2025.



# 02 Begriffsdefinitionen

**Network and Information Security Directive 2 (NIS 2)**

Mit der NIS-2-Richtlinie hat die Europäische Union den regulatorischen Rahmen für Cybersicherheit umfassend erweitert und verschärft. Als Weiterentwicklung der ursprünglichen NIS-Richtlinie aus dem Jahr 2016 verfolgt sie das Ziel, ein einheitlich hohes Sicherheitsniveau für Netz- und Informationssysteme innerhalb der EU zu schaffen.

In Deutschland erfolgt die Umsetzung durch das NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG), das am 6. Dezember 2025 in Kraft getreten ist. Die neuen Regelungen betreffen deutlich mehr Organisationen als bisher und erweitern sowohl die Anforderungen an das Risikomanagement als auch die Verantwortlichkeiten von Geschäftsleitungen und Führungskräften.

Kern der Richtlinie sind verbindliche Mindeststandards für technische, organisatorische und operative Sicherheitsmaßnahmen sowie erweiterte Meldepflichten für Sicherheitsvorfälle. Ziel ist es, die Resilienz von Unternehmen und kritischen Einrichtungen gegenüber Cyberbedrohungen nachhaltig zu stärken und die Sicherheit kritischer Dienstleistungen und Lieferketten zu gewährleisten.

Für betroffene Organisationen wird Cybersicherheit damit zu einer strategischen Managementaufgabe, die weit über reine IT-Schutzmaßnahmen hinausgeht und einen ganzheitlichen Ansatz aus Cyber-, Informations- und physischer Sicherheit erfordert.

**Critical Entities Resilience (CER)**

Die CER-Richtlinie soll die Resilienz der physischen Sicherheit stärken. Sie ist 2023 in Kraft getreten und wird in Deutschland über das KRITIS-Dachgesetz (KRITIS-DachG) umgesetzt. Das KRITIS-Dachgesetz legt Mindeststandards für den Schutz kritischer Infrastrukturen fest. Es verpflichtet Betreiber dazu, die Resilienz ihrer Systeme sicherzustellen.

Am 29.01.2026 wurde das KRITIS-Dachgesetz vom deutschen Bundestag verabschiedet. Am 17.03.2026 ist es offiziell in Kraft getreten.

**Der Cyber Resilience Act (CRA)**

ist die erste europaweite Regulierung, die verbindliche Cybersicherheitsanforderungen für Produkte mit digitalen Elementen definiert. Betroffen sind sowohl vernetzte als auch nicht vernetzte Produkte, sofern diese über digitale Schnittstellen verfügen.

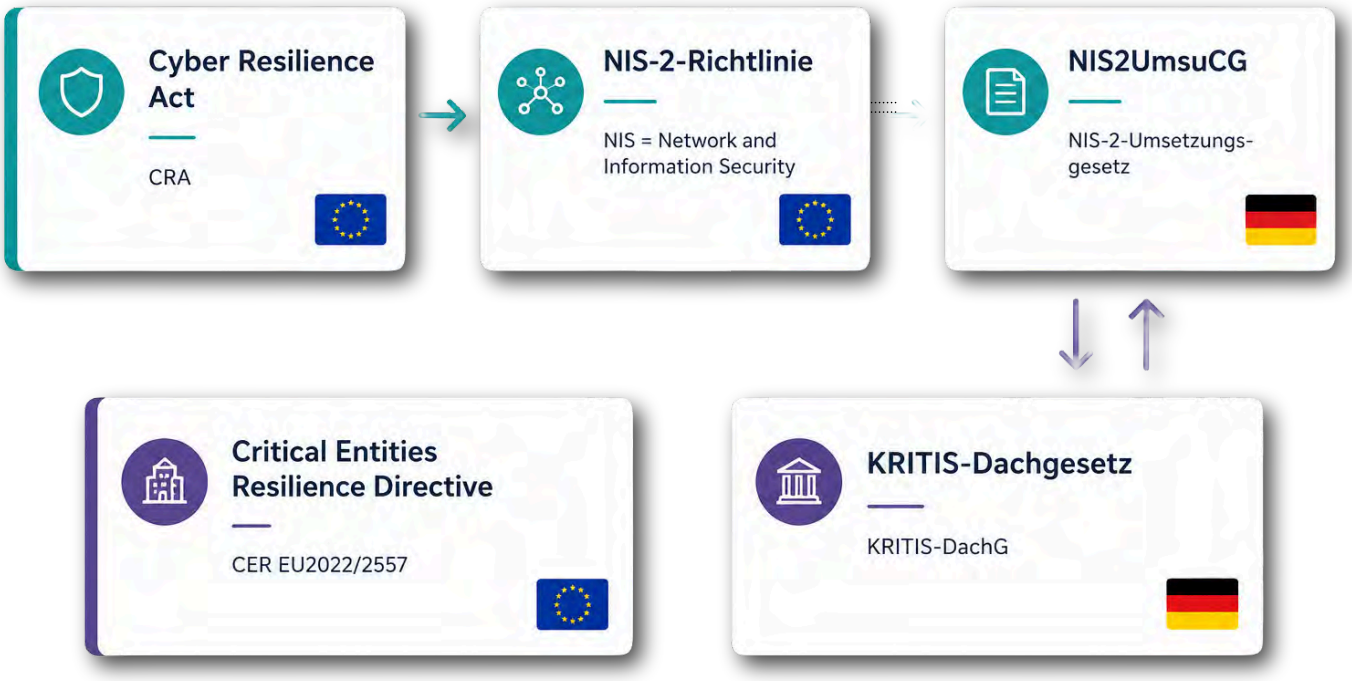
Die Verordnung ist am 10. Dezember 2024 in Kraft getreten. Erste Melde- und Berichtspflichten gelten ab dem 11. September 2026, bevor der CRA ab Dezember 2027 vollständig Anwendung findet.

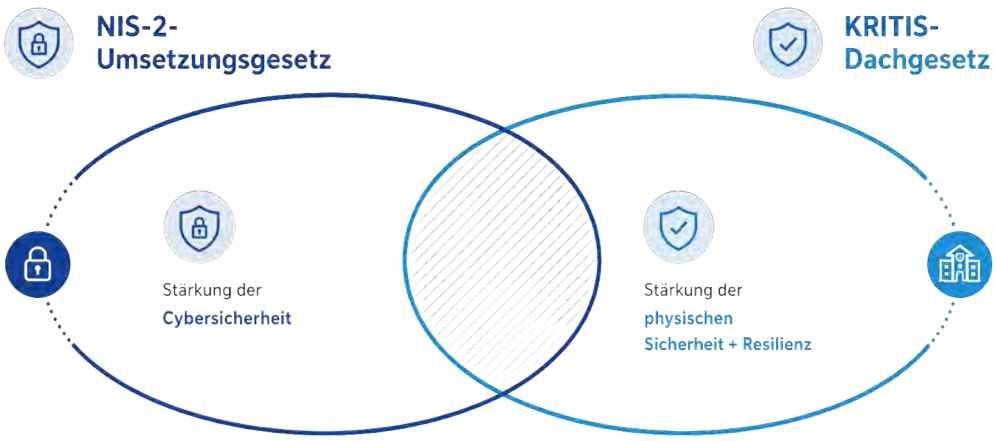
Besonders betroffen sind Hersteller von Hard- und Softwareprodukten. Sie müssen künftig nachweisen, dass ihre Produkte über den gesamten Lebenszyklus hinweg definierte Cybersicherheitsanforderungen erfüllen und angemessene Prozesse für das Schwachstellen- und Risikomanagement etabliert sind.

**Zusammenspiel von KRITIS-Dachgesetz und NIS 2**

Das KRITIS-Dachgesetz und das NIS-2-Umsetzungsgesetz bilden in Deutschland einen eng verzahnten regulatorischen Rahmen zur Stärkung der Resilienz kritischer Infrastrukturen. Beide Regelwerke verfolgen das gemeinsame Ziel, die Widerstandsfähigkeit von Organisationen gegenüber Krisen, Störungen und Angriffen nachhaltig zu erhöhen, setzen dabei jedoch unterschiedliche Schwerpunkte. Während NIS 2 primär die Cyber- und Informationssicherheit adressiert und Anforderungen an Risikomanagement, Sicherheitsmaßnahmen sowie Meldepflichten definiert, verfolgt das KRITIS-Dachgesetz einen deutlich umfassenderen Resilienzansatz. Es berücksichtigt neben der Informationssicherheit unter anderem auch Aspekte der physischen Sicherheit, des Krisen- und Notfallmanagements sowie organisatorische und personelle Vorsorgemaßnahmen.

Die Anforderungen der NIS-2-Regulierung sind dabei im KRITIS-Dachgesetz bereits berücksichtigt und bilden einen integralen Bestandteil der geforderten Resilienzmaßnahmen. Für Betreiber kritischer Infrastrukturen bedeutet dies, dass die Erfüllung von NIS 2 zwar eine wesentliche Grundlage schafft, für eine vollständige Compliance jedoch zusätzliche Anforderungen aus den Bereichen physische Sicherheit, Betriebsstabilität und Krisenvorsorge umgesetzt werden müssen. Ein wirksamer Compliance-Ansatz erfordert daher eine ganzheitliche Sicherheitsstrategie, die Cyber Security, Physical Security und organisatorische Resilienz gleichermaßen berücksichtigt.






**Cybersicherheit**

Cybersicherheit umfasst den Schutz von IT- und OT-Systemen, Netzwerken, Anwendungen sowie sensiblen Daten vor Cyberangriffen, Manipulationen, technischen Ausfällen und anderen digitalen Bedrohungen. Ziel ist es, die Verfügbarkeit, Integrität und Vertraulichkeit geschäftskritischer Systeme und Informationen sicherzustellen

Insbesondere im Umfeld vernetzter Gebäude und kritischer Infrastrukturen gewinnt der Schutz von Operational Technology (OT) – beispielsweise Gebäudeautomation, Sicherheits- und Steuerungssystemen – zunehmend an Bedeutung.

**Physische Sicherheit**

Physische Sicherheit umfasst alle Maßnahmen zum Schutz von Gebäuden, Anlagen, Infrastruktur und Sachwerten vor unbefugtem Zutritt, Diebstahl, Sabotage, Vandalismus und anderen physischen Bedrohungen. Zum Einsatz kommen dabei unter anderem Zutrittskontrollsysteme, Einbruchmeldeanlagen, Perimeterschutz, Videosicherheitssysteme sowie weitere organisatorische und technische Sicherheitsmaßnahmen. Ziel ist es, kritische Bereiche, Personen und Betriebsprozesse zuverlässig abzusichern und die Funktionsfähigkeit der Infrastruktur jederzeit zu gewährleisten.

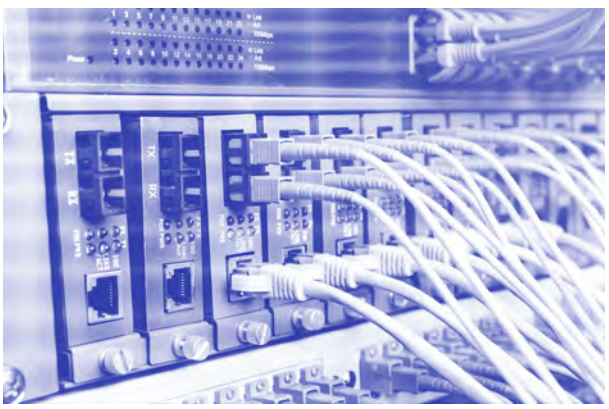
Der Schutz kritischer Infrastrukturen beginnt nicht erst im Netzwerk, sondern bereits an Gebäudegrenzen, Zugängen und sicherheitsrelevanten Anlagen. Resilienz entsteht durch das Zusammenspiel aus beiden Aspekten, denn erst die Verzahnung beider Disziplinen ermöglicht einen wirksamen Schutz vor modernen Bedrohungen.

**Überblick KRITIS-Dachgesetz**

Mit dem KRITIS-Dachgesetz schafft der Gesetzgeber erstmals einen sektorübergreifenden Rahmen zur Stärkung der Resilienz kritischer Infrastrukturen in Deutschland. Anders als viele bisherige Regulierungen beschränkt sich das Gesetz nicht auf die Informations- und Cybersicherheit, sondern verfolgt einen umfassenden Schutzansatz für kritische Einrichtungen und Dienstleistungen. Betroffen sind zahlreiche Sektoren, deren Ausfall erhebliche Auswirkungen auf Staat, Wirtschaft und Gesellschaft hätte. Dazu zählen unter anderem die Bereiche Energie, Transport und Verkehr, Finanzwesen, Gesundheitswesen, Wasser, Ernährung, Informationstechnik und Telekommunikation.

Zentrales Element des KRITIS-Dachgesetzes ist der sogenannte „All-Gefahren-Ansatz" (All Hazards Approach). Dieser berücksichtigt sämtliche relevanten Bedrohungsszenarien von Naturkatastrophen und technischen Störungen über menschliches Versagen bis hin zu Sabotage, Terrorismus oder gezielten Angriffen auf kritische Einrichtungen. Für Betreiber kritischer Infrastrukturen bedeutet dies, Risiken ganzheitlich zu betrachten und geeignete technische, organisatorische und physische Schutzmaßnahmen umzusetzen. Dabei müssen bestehende gesetzliche Vorgaben, branchenspezifische Standards sowie relevante Normen und Richtlinien in ein umfassendes Resilienz- und Sicherheitskonzept integriert werden.

Das KRITIS-Dachgesetz macht Resilienz damit zu einer strategischen Managementaufgabe und fordert einen ganzheitlichen Ansatz, der Cyber Security, Physical Security, Business Continuity und Krisenmanagement miteinander verbindet.



### 1. Strategisches Zielbild

Das KRITIS-Dachgesetz erweitert den Schutz kritischer Infrastrukturen über die reine IT-Sicherheit hinaus. Im Fokus steht die nachhaltige Stärkung der Resilienz gegenüber physischen Angriffen, Pandemien, Naturereignissen und weiteren systemischen Störungen. Ziel ist die Sicherung der kontinuierlichen Versorgungsfähigkeit kritischer gesellschaftlicher und wirtschaftlicher Prozesse.

### 2. Regulatorischer Fokus

Der Regelungsrahmen konzentriert sich auf vier zentrale Handlungsfelder:

- Erweiterte Meldepflichten bei sicherheitsrelevanten Ereignissen
- Anforderungen an physische Schutz- und Sicherheitsmaßnahmen
- Aufbau und Nachweis belastbarer Personal- und Krisenmanagementstrukturen
- Verstärkte behördliche Aufsicht und Koordination zwischen Bundes- und Landesebene

### 3. Aufsichts- und Behördenstruktur

Die Aufsicht wird institutionell erweitert und neu organisiert:

- Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) als zentrale Instanz im physischen Bevölkerungsschutz
- Bundesamt für Sicherheit in der Informationstechnik (BSI) weiterhin zuständig für IT-bezogene Resilienz
- Teilweise Einbindung der Landesbehörden zur operativen Umsetzung und Kontrolle

**Ergebnis:** integriertes Multi-Level-Governance-Modell

### 4. Anwendungsbereich und Adressaten

Betroffen sind Unternehmen aus zehn definierten Sektoren der kritischen Infrastruktur.
Als Orientierungsgröße gilt aktuell:

- Versorgung von mindestens 500.000 Personen

Eine Einstufung kann erfolgen durch:

- behördliche Identifikation

*oder*

- Risikoanalysen, insbesondere entlang kritischer Liefer- und Dienstleistungsketten

Auch indirekte Abhängigkeiten können zur Registrierungspflicht führen.

### 5. Geltung und Inkrafttreten

Das KRITIS-Dachgesetz ist am **17.03.2026** in Kraft getreten.Unternehmen sind verpflichtet, eigenständig zu prüfen, ob sie in den Anwendungsbereich fallen.

### 6. Fristen und Umsetzungsanforderungen

Nach Identifikation als potenziell KRITIS-relevant gelten verbindliche Zeitvorgaben:

*Registrierung*: innerhalb von 3 Monaten nach Identifizierung

*Risikoanalyse*: spätestens 9 Monate nach Registrierung, anschließend alle 4 Jahre

*Umsetzung Resilienzmaßnahmen*: innerhalb von 10 Monaten nach Registrierung

*Umsetzung Meldepflichten*: innerhalb von 10 Monaten nach Registrierung

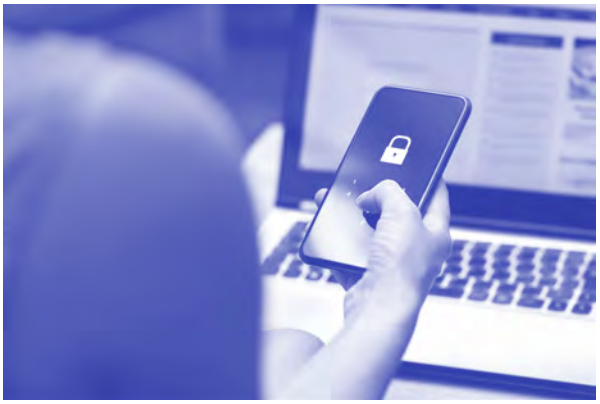
**NIS-2-Umsetzungsgesetz**

Das NIS-2-Umsetzungsgesetz erhöht die Anforderungen an die Cybersicherheit in Unternehmen und zielt darauf ab, bestehende Sicherheitslücken systematisch zu schließen sowie die Widerstandsfähigkeit gegenüber Cyberangriffen deutlich zu stärken. Der Anwendungsbereich wurde erweitert und umfasst nun sogenannte wichtige und besonders wichtige Einrichtungen aus insgesamt zehn Sektoren gemäß den Anlagen 1 und 2 des Bundesgesetzblatts.

Betroffene Unternehmen sind verpflichtet, umfassende technische und organisatorische Sicherheitsmaßnahmen umzusetzen, die auf einem risikobasierten Ansatz beruhen. Dazu zählen insbesondere ein strukturiertes IT-Risikomanagement, kontinuierliche Sicherheitsüberwachung sowie etablierte Prozesse für die Erkennung, Meldung und Bewältigung von Sicherheitsvorfällen.

Ein zentrales Element des Gesetzes ist die klare Verankerung von Verantwortung auf Führungsebene: Geschäftsleitungen tragen eine persönliche Haftung für die Umsetzung der Anforderungen und müssen deren Einhaltung aktiv sicherstellen und nachweisen. Zur Durchsetzung der Vorgaben sieht der Gesetzesentwurf zudem spürbare Sanktionen bei Verstößen vor, einschließlich hoher Geldbußen.

Insgesamt stellt das NIS-2-Umsetzungsgesetz einen deutlichen Ausbau der regulatorischen Anforderungen im Bereich der Cybersicherheit dar und verankert IT-Sicherheit verbindlich als strategische Managementaufgabe auf Unternehmensebene.



### 1. Strategisches Zielbild

Das NIS-2-Umsetzungsgesetz verfolgt das Ziel, ein europaweit einheitlich hohes Cybersicherheitsniveau in Deutschland und der EU zu etablieren. Es stellt eine Weiterentwicklung der NIS-1-Richtlinie dar und stärkt die digitale Resilienz von Unternehmen und kritischen digitalen Infrastrukturen nachhaltig.

### 2. Regulatorischer Fokus

Im Mittelpunkt stehen verbindliche Vorgaben für die Sicherheit von Netz- und Informationssystemen. Dazu gehören insbesondere verpflichtende Security-Richtlinien, Meldepflichten gegenüber dem BSI, ein strukturiertes Risikomanagement sowie Maßnahmen zur Absicherung der IT-Sicherheit entlang der gesamten Lieferkette.

### 3. Anwendungsbereich und Adressaten

Das Gesetz gilt für Unternehmen aus zehn Sektoren und unterscheidet zwei Kategorien:

Wichtige Einrichtungen: ≥ 50 Mitarbeitende oder ≥ 10 Mio. € Umsatz bzw. Bilanzsumme

Besonders wichtige Einrichtungen: ≥ 250 Mitarbeitende oder ≥ 50 Mio. € Umsatz bzw. ≥ 43 Mio. € Bilanzsumme

### 4. Gültigkeit

Das NIS-2-Umsetzungsgesetz ist am 06.12.2025 in Kraft getreten. Diese setzt die NIS-2-Richtlinie in deutsches Recht um und löst die bisherigen nationalen Regelungen ab.

### 5. Fristen und Umsetzungsanforderungen

Die Umsetzungspflichten gelten unmittelbar mit Inkrafttreten des Gesetzes. Unternehmen müssen die Anforderungen somit ohne Übergangsfrist vollständig erfüllen.

# 03 Anforderungen und Lösungen

Das KRITIS-Dachgesetz und das NIS-2-Umsetzungsgesetz verfolgen in weiten Teilen ein gemeinsames Ziel: die nachhaltige Erhöhung der Resilienz kritischer und wichtiger Infrastrukturen gegenüber physischen, organisatorischen und cyberbezogenen Bedrohungen. Während das KRITIS-Dachgesetz stärker auf physische Sicherheit, Krisenfestigkeit und betriebliche Resilienz ausgerichtet ist, fokussiert NIS-2 primär auf Cybersecurity und IT-Risikomanagement. Unternehmen, die unter das KRITIS-Dachgesetz fallen, sind grundsätzlich auch zur Einhaltung der NIS-2-Anforderungen verpflichtet. Umgekehrt gilt dies jedoch nicht: Viele „wichtige" und „besonders wichtige" Einrichtungen im Sinne von NIS-2 sind nicht automatisch vom KRITIS-Dachgesetz erfasst.

Im Folgenden werden drei zentrale Anforderungen aus beiden Regelwerken sowie typische Maßnahmen zur praktischen Umsetzung zusammengefasst:

**1. Risikoanalyse**

Die Risikoanalyse ist ein systematischer Prozess zur Identifikation, Bewertung und Priorisierung von Risiken, die sich auf eine Organisation, ein System oder einen Prozess auswirken können. Im Kontext von KRITIS und NIS-2 umfasst sie sowohl cyberbezogene als auch physische und organisatorische Risiken. Typische Umsetzungen beinhalten strukturierte Gefährdungsanalysen, Szenariobewertungen sowie die regelmäßige Überprüfung von Abhängigkeiten innerhalb kritischer Prozesse und Lieferketten.

**2. Risikomanagement und Resilienzfähigkeit**

Auf Basis der Risikoanalyse müssen Unternehmen ein kontinuierliches Risikomanagement etablieren, das Risiken aktiv steuert und die Resilienz der Organisation stärkt. Dazu zählen Maßnahmen zur Prävention, Detektion und Reaktion auf Störungen sowie die Absicherung geschäftskritischer Prozesse durch Business-Continuity-Management (BCM) und Notfallpläne.

### 3. Schutzmaßnahmen

Schutzmaßnahmen sind technische, organisatorische oder physische Vorkehrungen, die ergriffen werden, um Risiken zu minimieren, Systeme zu sichern und die Verfügbarkeit, Integrität sowie Vertraulichkeit von Daten und Infrastrukturen zu gewährleisten. Dazu gehören beispielsweise Zugriffskontrollen, Sicherheitsarchitekturen, physische Zugangssicherung, Redundanzkonzepte sowie organisatorische Sicherheitsrichtlinien.

### 4. Melde- und Kommunikationspflichten

Sicherheitsrelevante Vorfälle müssen zeitnah an die zuständigen Behörden gemeldet werden. Die Umsetzung erfolgt über definierte Incident-Response-Prozesse, standardisierte Eskalationswege sowie strukturierte Dokumentations- und Meldeverfahren.

### 5. Schutz von Systemen, Anlagen und Lieferketten

Beide Regelwerke verlangen den Schutz kritischer Systeme, Anlagen und abhängiger Lieferketten. Dies umfasst insbesondere die Absicherung von Dienstleistern, die Implementierung robuster IT- und Sicherheitsarchitekturen sowie Maßnahmen zur Sicherstellung der Betriebskontinuität auch bei Störungen oder Angriffen.

**NIS-2-Umsetzungsgesetz**

Im Rahmen von NIS-2 erfolgt die Meldung zentral an das Bundesamt für Sicherheit in der Informationstechnik (BSI). Die wesentlichen Anforderungen umfassen:

- Erstmeldung innerhalb von 24 Stunden nach Feststellung eines Vorfalls
- Bestätigung und Bewertung des Vorfalls inklusive Schweregradeinschätzung innerhalb von 72 Stunden
- Möglichkeit einer Zwischenmeldung auf Anforderung des BSI
- Erstellung eines ausführlichen Abschlussberichts innerhalb eines Monats

**KRITIS-Dachgesetz**

Das KRITIS-Dachgesetz fokussiert stärker auf erhebliche Betriebsstörungen und physische sowie organisatorische Auswirkungen. Die Anforderungen umfassen:

- Meldung von Vorfällen mit erheblicher Betriebsbeeinträchtigung
- Zuständige Kontaktstelle: gemeinsames Meldesystem von BBK und BSI
- Erstmeldung in der Regel innerhalb von 24 Stunden
- Ausgestaltung und Detailtiefe der Meldungen abhängig von den Vorgaben der zuständigen Behörden
- Frist zur Umsetzung organisatorischer Meldeprozesse: 10 Monate nach Registrierung
- Mögliche Sicherheitsmaßnahmen zur Umsetzung der Meldepflichten

**Sicherheitsinfrastruktur**

Einrichtung moderner Sicherheits- und Kommunikationsstrukturen zur schnellen Vorfallserkennung und -meldung, einschließlich definierter Rollen, klarer Eskalationswege sowie zentraler Notruf- und Servicestellen.

**Meldepflichten**

Beide Regelwerke verpflichten Unternehmen zur Meldung sicherheitsrelevanter Vorfälle an zuständige Behörden. Im Fokus steht dabei eine schnelle Reaktionsfähigkeit sowie eine strukturierte, nachvollziehbare Dokumentation von Sicherheitsereignissen. Das NIS-2-Umsetzungsgesetz sieht dabei besonders kurze Reaktionszeiten vor.

## Resilienzanforderungen

Im Falle von Störungen sowie Cyber- oder physischen Angriffen verlangen sowohl das KRITIS-Dachgesetz als auch das NIS-2-Umsetzungsgesetz die Umsetzung geeigneter Maßnahmen zur Sicherstellung des Betriebs und zur schnellen Wiederherstellung kritischer Prozesse und Infrastrukturen. Ziel ist eine signifikante Erhöhung der organisatorischen, technischen und physischen Resilienz betroffener Unternehmen.

Die zentralen Anforderungen unterscheiden sich dabei in ihrer Schwerpunktsetzung:

**NIS-2-Umsetzungsgesetz**

- Einhaltung des aktuellen Stands der Technik
- Etabliertes Incident Management
- Business Continuity Management (BCM)
- Sensibilisierung, Schulung und regelmäßiges Training der Mitarbeitenden
- Absicherung der Lieferkette (Supply Chain Security)
- Notfallpläne inklusive Notfallkommunikation und Krisenreaktion

**KRITIS-Dachgesetz**

- Physischer Schutz von Anlagen und Infrastrukturen
- Maßnahmen zur Reaktion, Abwehr und Eindämmung von Vorfällen
- Folgenbegrenzung und Schadensminimierung
- Wiederherstellung kritischer Funktionen
- Schulungen und regelmäßige Übungen zur Krisenvorsorge
- Konkrete Maßnahmen gemäß § 13 Abs. 3
- Abbildung in einem strukturierten Resilienzplan
- Orientierung an branchenspezifischen Resilienzstandards
- Umsetzung innerhalb von 10 Monaten nach Registrierung

Insgesamt ergänzen sich beide Regelwerke zu einem ganzheitlichen Sicherheitsansatz, der sowohl präventive als auch reaktive Maßnahmen umfasst und Unternehmen auf eine dauerhaft hohe Widerstandsfähigkeit gegenüber unterschiedlichen Bedrohungslagen ausrichtet.

## Mögliche Sicherheitsmaßnahmen

Im Kontext von KRITIS-Dachgesetz und NIS-2-Umsetzungsgesetz stehen Maßnahmen zur Sicherstellung der Betriebsfähigkeit und zur schnellen Wiederherstellung nach Störungen, Cyberangriffen oder physischen Angriffen im Mittelpunkt. Ziel ist der Aufbau einer robusten, widerstandsfähigen Infrastruktur, die auch unter Krisenbedingungen funktionsfähig bleibt.

**Ausfallsicherheit**

Aufbau und Betrieb von Redundanzen für kritische Infrastrukturen und IT-Systeme zur Vermeidung von Single Points of Failure. Dazu zählen insbesondere:

1

- Notstromversorgungen und unterbrechungsfreie Energieversorgung
- Ausweich- und Ersatzstandorte (Failover-Infrastruktur)
- Redundante System- und Netzwerkarchitekturen
- Cloud-Backups und georedundante Datensicherung

**Notfallmanagement**

Strukturierte Prozesse zur schnellen Reaktion und Wiederherstellung nach sicherheitsrelevanten Vorfällen. Im Fokus stehen:

2

- Entwicklung und regelmäßige Durchführung von Notfall- und Krisenplänen
- Etabliertes Business-Continuity-Management (BCM)
- Incident-Response-Pläne (IRP) zur koordinierten Vorfallbearbeitung
- Definition klarer Vorgehensweisen bei identifizierten Schwachstellen
- Regelmäßige Tests von Backup- und Restore-Prozessen zur Sicherstellung der Wiederherstellbarkeit

**Schutz- und Abwehrmaßnahmen**

Implementierung integrierter physischer und cyberbezogener Sicherheitsmaßnahmen zur Prävention und Eindämmung von Angriffen:

Physische Sicherheit:

3

- Einbruchmeldeanlagen
- Perimeterschutzsysteme
- Zutrittskontrollsysteme
- Videoüberwachungssysteme

**Cybersicherheit:**

4

- Ganzheitliche Sicherheitsarchitekturen mit Netzwerksegmentierung
- Verschlüsselung sensibler Daten und Kommunikation
- Network Access Control (NAC)
- Multi-Faktor-Authentifizierung (MFA)
- Single Sign-On (SSO)

**Vorfallsdokumentation**

Systematische und vollständige Dokumentation aller sicherheitsrelevanten Ereignisse, einschließlich Ursachenanalyse, betroffener Systeme sowie eingeleiteter Gegenmaßnahmen.

5

**Vorfall-Reporting**

Sicherstellung eines kontinuierlichen Reportings an interne und externe Stakeholder, inklusive regelmäßiger Updates, Lageeinschätzungen sowie Darstellung der Auswirkungen und eingeleiteten Korrekturmaßnahmen.

6

# 04 Ganzheitlicher Schutz

Die Umsetzung der Anforderungen aus dem KRITIS-Dachgesetz und der NIS-2-Richtlinie erfordert ein breites Spektrum an Maßnahmen – von Perimeterschutz und Zutrittskontrolle über Videoüberwachung bis hin zu Cybersicherheit und Sicherheitsmanagement.

Viele Unternehmen setzen dabei auf unterschiedliche Einzellösungen und Dienstleister. Dies kann zu erhöhtem Koordinationsaufwand, Medienbrüchen und einer uneinheitlichen Sicherheitsarchitektur führen.

Ein integrierter Sicherheitsansatz ermöglicht es hingegen, physische Sicherheit, Cybersicherheit und organisatorische Prozesse aufeinander abzustimmen. Dadurch lassen sich regulatorische Anforderungen effizienter umsetzen, Sicherheitslücken reduzieren und betriebliche Abläufe vereinfachen.

Novatec Europe unterstützt Betreiber kritischer Infrastrukturen dabei, Sicherheits- und Resilienzanforderungen strukturiert in bestehende Betriebs- und Sicherheitslandschaften zu integrieren. Ziel ist die nachhaltige Absicherung geschäftskritischer Prozesse sowie die Stärkung der organisatorischen und technischen Resilienz gegenüber aktuellen und zukünftigen Bedrohungen.

# 05 Jetzt handeln – nächste Schritte zur Umsetzung

Für Betreiber kritischer Infrastrukturen ist es entscheidend, die Anforderungen des KRITIS-Dachgesetzes und des NIS2UmsuCG strukturiert und frühzeitig in konkrete Maßnahmen zu überführen. Ausgangspunkt hierfür ist eine belastbare Einschätzung des aktuellen Sicherheitsniveaus über alle relevanten Bereiche hinweg – von IT und OT über Prozesse bis hin zur organisatorischen Verankerung.

Strukturierte Standortbestimmung durch KRITIS-Expertise
Novatec Europe unterstützt Unternehmen dabei, genau diese Ausgangsbasis zu schaffen – nicht über standardisierte Selbsttests, sondern durch fundierte Analyse- und Beratungsleistungen unserer KRITIS-Experten.

Transparenz über Risiken und konkrete Handlungsfelder
Das Ergebnis ist eine klare, nachvollziehbare Einschätzung des aktuellen Sicherheitsniveaus sowie der bestehenden Lücken in der Sicherheitsarchitektur. Auf dieser Basis erhalten Unternehmen praxisnahe und priorisierte Handlungsempfehlungen, die als Grundlage für die gezielte Umsetzung regulatorischer Anforderungen dienen.

So entsteht ein strukturierter Einstieg in die KRITIS- und NIS2-Compliance – mit dem Ziel, Risiken transparent zu machen, Maßnahmen gezielt zu priorisieren und die Resilienz der kritischen Infrastruktur nachhaltig zu stärken.


Von der ersten Einschätzung bis zur Umsetzung konkreter Maßnahmen: Wir unterstützen Sie dabei, Risiken zu erkennen, Anforderungen zu erfüllen und Ihre Sicherheitsstrategie nachhaltig zu stärken. Kontaktieren Sie uns für eine unverbindliche Erstberatung.

**+49 171 2769228**
**kontakt@novatec.email**
**www.novatec-europe.net**

# 06 Ausblick

Die dargestellten Beispiele unterstreichen die zentrale Bedeutung eines durchgängig ganzheitlichen Sicherheitsansatzes. Erst das Zusammenspiel aus umfassenden Schutzmaßnahmen, kontinuierlicher Überwachung und einer hohen Reaktionsfähigkeit ermöglicht eine wirksame Abwehr moderner Bedrohungsszenarien – über die Grenzen von physischer Sicherheit und Cybersicherheit hinweg.

Für KRITIS-Betreiber sollten die gesetzlichen Anforderungen dabei nicht primär als regulatorische Zusatzlast verstanden werden, sondern als strategischer Hebel zur nachhaltigen Stärkung der eigenen Resilienz. Die konsequente Umsetzung integrierter Sicherheitsmaßnahmen erhöht nicht nur den Schutz vor zunehmenden und zunehmend komplexen Angriffen, sondern führt zugleich zu einer Optimierung von Technologien, Prozessen und organisatorischen Abläufen.
Dies trägt maßgeblich zur Reduktion potenzieller Ausfallzeiten in Produktion und Betrieb bei und stärkt damit die betriebliche Stabilität. Darüber hinaus entsteht ein klarer Mehrwert über die Compliance hinaus: gesteigertes Vertrauen bei Kunden, Partnern und Stakeholdern durch nachweislich belastbare Sicherheits- und Resilienzstrukturen.

**Herausgegeben von**
Novatec Germany GmbH
An Der Pönt t 67-71 | D-40885 Ratingen
www.novatec-europe.net