NIS-2 Richtlinie: Wesentliche Definitionen, Pflichten, Bußgelder für Unternehmen (ohne Verwaltung)

www.massandra-eBusiness.com

👉 Betreiber kritischer Anlagen

Die Sektoren für Betreiber kritischer Anlagen sind separat zu den Einrichtungen und sowohl in der NIS-2 Richtlinie als auch im KRITIS-Dachgesetz definiert.
Kritische Anlagen sind solche, deren Ausfall oder Beeinträchtigung erhebliche Auswirkungen auf die Versorgungssicherheit oder die öffentliche Sicherheit haben könnte. Die kritischen Dienstleistungen und Anlagen müssen teilweise noch in einer Verordnung festgelegt werden. Das KRITIS Dachgesetz ist noch in Bearbeitung.
Schwellenwerte für kritische Anlagen werden in der "Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz" BSI-KritisV festgelegt.

👉 **KRITIS Schwellenwerte:** Sie gehören zu einem Betreiber kritischer Anlagen entsprechend der Anlagenkategorien, wenn ein Schwellenwert überschrittenen wird.

👉 Betreiber kritischer Anlagen haben sowohl das KRITIS-Dachgesetzes als auch die NIS-2 Richtlinie einzuhalten.
Betreiber kritischer Anlagen werden unabhängig von der Unternehmensgröße immer als eine besonders wichtige Einrichtungen und als Betreiber einer kritischen Anlage reguliert.

Besonders wichtige Einrichtung

👉 Betreiber kritischer Anlagen

👉 Qualifizierte Vertrauensdiensteanbieter, Top Level Domain Name Registries oder DNS-Diensteanbieter

👉 Anbieter öffentlich zugänglicher Telekommunikationsdienste oder Betreiber öffentlicher Telekommunikationsnetze, die
a) mindestens 50 Mitarbeiter beschäftigen oder
b) einen Jahresumsatz und eine Jahresbilanzsumme von jeweils über 10 Millionen Euro aufweisen;

👉 Natürliche oder juristische Personen, die anderen natürlichen oder juristischen Personen entgeltlich Waren oder Dienstleistungen anbieten, die einer der in **Anlage 1** bestimmten Einrichtungsarten zuzuordnen sind und die
a) mindestens 250 Mitarbeiter beschäftigt oder
b) einen Jahresumsatz von über 50 Millionen Euro und eine Jahresbilanzsumme von über 43 Millionen Euro aufweisen.

Wichtige Einrichtung

👉 Vertrauensdiensteanbieter

👉 Anbieter öffentlich zugänglicher Telekommunikationsdienste oder Betreiber öffentlicher Tele kommunikationsnetze, die
a) weniger als 50 Beschäftigte haben und
b) einen Jahresumsatz und eine Jahresbilanzsumme von jeweils 10 Millionen Euro oder weniger aufweisen.

👉 Natürliche oder juristische Personen, die anderen natürlichen oder juristischen Personen entgeltlich Waren oder Dienstleistungen anbietet, die einer der in **Anlagen 1 und 2** bestimmten Einrichtungsarten zuzuordnen sind und die
a) mindestens 50 Mitarbeiter beschäftigt oder
b) einen Jahresumsatz und eine Jahresbilanzsumme von jeweils über 10 Millionen Euro auf weisen.

NIS-2 Richtinie Deutschland

Referentenentwurf vom 2.10.2024

Sektoren Kritis: Betreiber kritischer Anlagen

1. Energie
2. Transport und Verkehr
3. Finanz- und Versicherungsleistungen
4. Gesundheit
5. Ernährung
6. Informationstechnik und Telekommunikation
7. Siedlungs-Abfallentsorgung
8. Wasser

NIS-2 Sektoren Anlage 1

1. Energie
2. Transport und Verkehr
3. Finanzwesen
4. Gesundheit
5. Wasser
6. Digitale Infrastruktur
7. Weltraum

NIS-2 Sektoren Anlage 2

1. Transport und Verkehr: Post- und Kurierdienste
2. Abfallbewirtschaftung
3. Produktion, Herstellung und Handel mit chemischen Stoffen
4. Produktion, Verarbeitung und Vertrieb von Lebensmitteln
5. Verarbeitendes Gewerbe/Herstellung von Waren
6. Anbieter digitaler Dienste
7. Forschung

Aussnahmen und erweiterte Pflichten:

1. DORA, TKG, EnWG regulierte Unternehmen
2. Betreiber von Internet Exchange Points
3. DNS-Dienstanbieter
4. Top Level Domain Name Registry
5. Anbieter von Cloud-Computing-Diensten
6. Anbieter von Rechenzentrumsdiensten
7. Betreiber von Content Delivery Networks
8. Managed Services Provider
9. Managed Security Services Provider
10. Anbieter von Online-Marktplätzen
11. Online-Suchmaschinen
12. Plattformen für Dienste sozialer Netzwerke
13. Anbieter öffentlich zugänglicher elektronsicher Kommunikationsdienste

👉 Zusätzliche Pflichten für Betreiber kritscher Anlagen

§ 31 Besondere Anforderungen an die Risikomanagementmaßnahmen
§ 32 Meldepflichten
§ 33 Registrierungspflicht
§ 34 Besondere Registrierungspflicht für bestimmte Einrichtungsarten
§ 35 Unterrichtungspflichten
§ 39 Nachweispflichten für Betreiber kritischer Anlagen
§ 41 Untersagung des Einsatzes kritischer Komponenten

👉 § 65 Bußgeldvorschriften

- Wichtige Einrichtungen: Von 100.000 EUR bis zu 7 Mio EUR Bußgelder (oder bis zu 1,4 Prozent des Jahresumsatzes) je nach Zuwiderhandlung.
- Besonders wichtige Einrichtungen: Von 100.000 EUR bis zu 10 Mio EUR Bußgelder (oder bis zu 2 Prozent des Jahresumsatzes) je nach Zuwiderhandlung

👉 §§ 61,62 Durchsetzungsmaßnahmen

- Anordnung von Audits, Prüfungen oder Zertifizierungen
- Festlegung fachlicher und organisatorischer Anforderungen
- Überprüfung der Einhaltung der Anforderungen
- Anordnung von Maßnahmen zur Verhütung oder Behebung eines Sicherheitsvorfalls
- Unterrichtung über Cyberbedrohungen
- Öffentliche Bekanntmachung von Verstößen
- Mitteilung an die zuständige Aufsichtsbehörde
- Aussetzung der Genehmigung und Untersagung der Tätigkeit

👉 § 30 Risikomanagementmaßnahmen besonders wichtiger Einrichtungen und wichtiger Einrichtungen

- Konzepte in Bezug auf die Risikoanalyse und auf die Sicherheit in der Informationstechnik.
- Bewältigung von Sicherheitsvorfällen.
- Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement.
- Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern.
- Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von informationstechnischen Systemen, Komponenten und Prozessen, einschließlich Management und Offenlegung von Schwachstellen.
- Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Sicherheit in der Informationstechnik.
- Grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Sicherheit in der Informationstechnik.
- Konzepte und Verfahren für den Einsatz von Kryptografie und Verschlüsselung.
- Sicherheit des Personals, Konzepte für die Zugriffskontrolle und für das Management von Anlagen.
- Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung.

👉 §§ 32, 35 Meldepflichten, Unterrichtungspflichten

Besonders wichtige Einrichtungen und wichtige Einrichtungen sind gemäß der NIS2-Regulierung verpflichtet, erhebliche Sicherheitsvorfälle unverzüglich zu melden und die Empfänger ihrer Dienste über solche Vorfälle zu informieren. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) bietet Rückmeldungen und Unterstützung bei der Bewältigung der Vorfälle: Innerhalb von 24 Stunden nach Kenntniserlangung, innerhalb von 72 Stunden nach Kenntniserlangung Aktualisierung der Meldung. Auf Ersuchen des Bundesamtes Zwischenmeldung, spätestens einen Monat nach Übermittlung der Meldung des Sicherheitsvorfalls eine Abschlussmeldung.

👉 § 33 Registrierungspflicht

Besonders wichtige und wichtige Einrichtungen müssen sich spätestens drei Monate, nachdem sie erstmals oder erneut als solche gelten, beim Bundesamt registrieren. Die Registrierung erfolgt über eine gemeinsam vom Bundesamt (BSI) und dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe eingerichtete Registrierungsmöglichkeit. Diese Registrierung beinhaltet grundlegende Informationen wie z.B. Namen, Kontaktdaten und den Sektor der Einrichtung.

👉 § 38 Pflichten der Geschäftsleitungen besonders wichtiger Einrichtungen und wichtiger Einrichtungen

- Geschäftsleitungen sind verpflichtet, die von diesen Einrichtungen nach § 30 zu ergreifenden Risikomanagementmassnahmen umzusetzen und ihre Umsetzung zu überwachen.
- Geschäftsleitungen, die ihre Pflichten nach Absatz 1 verletzen, haften ihrer Einrichtung für einen schuldhaft verursachten Schaden nach den auf die Rechtsform der Einrichtung anwendbaren Regeln des Gesellschaftsrechts. Nach diesem Gesetz haften sie nur, wenn die für die Einrichtung maßgeblichen gesellschaftsrechtlichen Bestimmungen keine Haftungsregelung enthalten.
- Die Geschäftsleitungen müssen regelmäßig an Schulungen teilnehmen, um ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken und von Risikomanagementpraktiken im Bereich der Sicherheit in der Informationstechnik zu erlangen sowie um die Auswirkungen von Risiken sowie Risikomanagementpraktiken auf die von der Einrichtung erbrachten Dienste beurteilen zu können.