

Statement des Managements der SBF AG zu KRITIS und NIS-2

Nachhaltiges und verantwortungsvolles Handeln auch unter dem Aspekt der IT- und physischen Sicherheit ist ein zentraler Bestandteil unserer Unternehmensstrategie. Als mittelständisches Unternehmen im produzierenden Gewerbe sehen wir es als unsere Verantwortung, ökonomischen Erfolg mit ökologischer, sicherheitstechnischer und sozialer Verantwortung, sowie guter Unternehmensführung in Einklang zu bringen.

Kurzbeschreibung des Unternehmens

- Die SBF-Gruppe umfasst Spezialisten für innovative Lösungen in den Bereichen Schienenfahrzeuge, Beleuchtung, Elektromechanik und Sensorik. In der Unternehmensgruppe bündeln hochspezialisierte und in ihren Bereichen führende Hidden Champions ihre Expertise. Mit einem hochwertigen und zukunftsweisenden Produkt- und Serviceportfolio profitiert SBF von den Megatrends Mobilität, Klimaschutz, Automatisierung und Digitalisierung sowie von Security-Lösungen für kritische Infrastrukturen und Defense-Anwendungen. Zusätzlich verfügen wir über qualifizierte Kapazitäten im Bereich Entwicklung und Engineering sowie in der Produktion zur lokalen Fertigung kritischer Komponenten, insbesondere vor dem Hintergrund gestörter Lieferketten.
- Im Geschäftsfeld „Schienenfahrzeuge“ beliefert der Tier-1-Systemlieferant und Entwicklungspartner die weltweit führenden Schienenfahrzeughersteller mit komplexen Interior-, Decken- und Beleuchtungssystemen „Made in Germany“.
- Das Geschäftsfeld „Öffentliche und Industrielle Beleuchtung“ umfasst intelligente und maßgeschneiderte LED-Systeme zur effizienten Beleuchtung industrieller, kommunaler und infrastruktureller Projekte.
- Zudem werden im Geschäftsfeld „Sensortechnologie und Elektromechanik“ zukunftsweisende Komponenten und Software für elektromechanische Produkte wie Platinen, Sensoren und Kommunikationstechnologien entwickelt und produziert.

Weitere Informationen unter <https://www.sbf-ag.com>.

Die KRITIS-Belange, im Umfang ihrer Relevanz für unser Unternehmen, sind in unserem QM-Handbuch integriert. Maßnahmen und Updates werden regelmäßig aktualisiert.

Das KRITIS-Thema hat auch Relevanz für unsere Vertragspartner, daher haben wir wesentliche Eckpunkte zusammengefasst, um das Risiko für die Vertragspartner zu reduzieren.

Der Pflichtenkatalog des KRITIS-Dachgesetzes

Das Gesetz folgt einem All-Gefahren-Ansatz. Es schützt nicht vor einem spezifischen Szenario, sondern fordert Resilienz gegenüber Naturgefahren (Klimawandel), technischem Versagen und menschlichen Angriffen (Sabotage, Terrorismus). Adressat des Gesetzes ist der Betreiber einer kritischen Anlage.

Die zentralen Verpflichtungen lassen sich in vier Säulen gliedern:

1. **Registrierung und Identifikation (§ 16 KRITIS-DachG-E)**
Betreiber müssen ihre Anlagen eigenständig identifizieren und beim Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) registrieren. Dies schafft erstmals ein umfassendes Kataster kritischer Anlagen in Deutschland.
2. **Risikoanalyse (§ 12 KRITIS-DachG-E)**
Alle vier Jahre ist eine umfassende Risikoanalyse durchzuführen. Diese muss auf der Nationalen Risikoanalyse des Bundes aufbauen und lokale Gefährdungen bewerten.

Hierbei sind Abhängigkeiten von anderen Sektoren (z. B. Strom, Wasser) explizit zu berücksichtigen.

3. Resilienzmaßnahmen und Resilienzplan (§ 13 KRITIS-DachG-E)

Herzstück des Gesetzes ist die Pflicht, „geeignete und verhältnismäßige“ Maßnahmen zu treffen. Diese sind in einem Resilienzplan zu dokumentieren. Der Maßnahmenkatalog umfasst u. a.:

- **Baulich/Technisch:** Zäune, Vereinzelungsanlagen, Härtung der Gebäudehülle, Notstromversorgung, Detektionstechnik.
- **Organisatorisch:** Krisenmanagement, Business Continuity Management (BCM), Überprüfung von Personal.

4. Meldewesen (§ 18 KRITIS-DachG-E)

Störfälle, die die Erbringung der kritischen Dienstleistung erheblich beeinträchtigen können, sind unverzüglich (binnen 24 Stunden) an die gemeinsame Meldestelle von BBK und BSI zu melden.

Die KRITIS-Regulierung ist fragmentiert und umfasst diverse unterschiedliche Normen auf gesetzlicher und untergesetzlicher Ebene (siehe hierzu die Erläuterungen zum Aufbau des NIS-2-Umsetzungsgesetzes). Im Folgenden finden Sie eine Übersicht der wichtigsten Normen, Begründungen und Auslegungshinweise für die Ver- und Entsorgungswirtschaft.

Alle Fassungen des **NIS-2-Umsetzungsgesetzes** und des **KRITIS-Dachgesetzes (KRITIS-DachG)** finden Sie unter den Normentwürfen / Normbegründungen weiter unten.

Normen

Deutsche Gesetze

- [NIS-2-Umsetzungsgesetz](#)
 - [BSIG](#)
 - [EnWG](#) (insbesondere §§ 5c - 5e EnWG)
 - [TKG](#) (insbesondere §§ 165 - 168 TKG)
- KRITIS-DachG (siehe zum aktuellen Stand unten)
- Allgemeine Gesetze
 - [AktG](#) (insbesondere § 93 AktG)
 - [GmbHG](#) (insbesondere § 43 GmbHG)

Deutsche untergesetzliche Normen

- [BSI-Kritisverordnung](#)
- IT-Sicherheitskataloge
 - [Betreiber von Energienetzen](#)
 - [Betreiber von Energieanlagen](#)
 - [Betreiber von TK-Infrastrukturen](#)

Europäische Gesetze und Verordnungen

- [NIS2-Richtlinie \(Richtlinie \(EU\) 2022/2555 vom 14. Dezember 2022\)](#)
- [CER-Richtlinie \(Richtlinie \(EU\) 2022/2557 vom 14. Dezember 2022\)](#)
- [Delegierte Verordnung \(EU\) 2023/2450 zur Ergänzung CER-Richtlinie durch eine Liste wesentlicher Dienste](#)
- [Delegierte Verordnung \(EU\) 2024/1366 - Netzkodex mit sektorspezifischen Vorschriften für Cybersicherheitsaspekte grenzüberschreitender Stromflüsse](#)
- [Durchführungsverordnung \(EU\) 2024/2690](#) (spezifische Anforderungen an IKT-Betreiber)
- [Cyber Resilience Act](#) (Cybersicherheitspflichten hauptsächlich für Hersteller von Produkten mit digitalen Elementen)

Normentwürfe / Normbegründungen

NIS-2-Umsetzungsgesetz (2025)

- Beschlussempfehlung und Bericht Innenausschuss im Bundestag (Änderungen am Gesetzentwurf der Bundesregierung durch den Bundestag; Stand: 12.11.2025)

NIS-2

1. Ziel der NIS-2

Das Hauptziel ist es, ein hohes gemeinsames Cybersicherheitsniveau in der EU zu gewährleisten, insbesondere für kritische und wichtige Organisationen. Angesichts zunehmender Cyberangriffe soll die Resilienz von Wirtschaft und Staat verbessert werden.

2. Erweiterter Anwendungsbereich

NIS-2 gilt für deutlich mehr Organisationen als zuvor. Sie unterscheidet zwei Kategorien:

- **Wesentliche Einrichtungen (Essential Entities)**
z. B. Energie, Verkehr, Gesundheitswesen, Trinkwasser, digitale Infrastruktur, öffentliche Verwaltung
- **Wichtige Einrichtungen (Important Entities)**
z. B. Post- und Kurierdienste, Abfallwirtschaft, Chemieindustrie, Lebensmittelproduktion, IT-Dienstleister

Maßgeblich sind meist Branche und Unternehmensgröße, nicht mehr nur „kritische Infrastruktur“.

3. Verbindliche Sicherheitsmaßnahmen

Betroffene Organisationen müssen konkrete technische und organisatorische Maßnahmen umsetzen, u. a.:

- Risikomanagement und Sicherheitskonzepte
- Incident-Handling (Erkennen, Reagieren, Wiederherstellen)
- Backup- und Krisenmanagement

Was müssen Unternehmen im Rahmen der NIS-2 leisten?

Die Einführung der Network and Information Security 2 (NIS-2) - Richtlinie bringt für Unternehmen eine Vielzahl neuer Pflichten und Anforderungen mit sich.

Zunächst muss ein Unternehmen sich selbst in die unterschiedlichen Stufen einordnen (z. B. „besonders wichtige Einrichtung“ oder „wichtige Einrichtung“) und sich beim Bundesamt für Sicherheit in der Informationstechnik (BSI) innerhalb von drei Monaten nach Identifikation registrieren. „Besonders wichtige“ Einrichtungen müssen am Informationsaustausch über die zentrale Austauschplattform des BSI (BISP) teilnehmen.

Neben der Registrierung bei der zuständigen Behörde im eigenen Mitgliedsstaat und der Meldung von Sicherheitsvorfällen müssen sich Unternehmen insbesondere mit den neuen, strengen Sicherheitsanforderungen im Rahmen von NIS-2 auseinandersetzen.

1. Risikomanagement als Grundpfeiler der NIS-2-Compliance etablieren

Ein zentraler Aspekt ist ein NIS-2-konformes Risikomanagement für die Informationssicherheit.

Unternehmen, die als wesentliche oder wichtige Einrichtungen eingestuft werden, sind verpflichtet, angemessene und verhältnismäßige technische, operative und organisatorische Maßnahmen zu ergreifen, um Risiken für die Sicherheit ihrer Netz- und Informationssysteme zu beherrschen und die Auswirkungen von Sicherheitsvorfällen zu verhindern oder zu minimieren. Die NIS-2-Richtlinie fordert somit auch technische und organisatorische Maßnahmen (TOM) gemäß dem sogenannten „Stand der Technik“.

Durch ein strukturiertes Risikomanagement können Unternehmen potenzielle Bedrohungen und Schwachstellen in ihren Netz- und Informationssystemen frühzeitig erkennen. Dies umfasst sowohl interne als auch externe Bedrohungen, wie etwa Cyberangriffe, Datenschutzverletzungen, Systemausfälle oder menschliches Fehlverhalten.

Ein systematisches Risikomanagement führt insgesamt zu einer erhöhten Widerstandsfähigkeit gegenüber Bedrohungen und Angriffen.

Indem Unternehmen ihre Risiken strukturiert analysieren und bewerten, können sie gezielte Maßnahmen zur Reduzierung identifizierter Schwachstellen ergreifen. Dadurch sind sie besser auf mögliche Angriffe vorbereitet und in der Lage, schneller und effektiver auf Sicherheitsvorfälle zu reagieren. Das Ergebnis ist eine geringere Anfälligkeit für Cyberangriffe und eine verbesserte Fähigkeit zur Abwehr und Schadensbegrenzung.

Würde diese Praxis flächendeckend umgesetzt, entstünde ein kohärentes Sicherheitsniveau, das die europäische Infrastruktur nachhaltig schützen und stärken kann.

2. Informationssicherheitsstandards in Lieferketten sicherstellen

Die Sicherheit in der Lieferkette ist ein wichtiger Aspekt der NIS-2-Anforderungen. Unternehmen müssen sicherstellen, dass auch ihre Geschäftspartner und Dienstleister angemessene Sicherheitsvorkehrungen im Bereich der Informationssicherheit treffen. Dies kann beispielsweise durch vertragliche Vereinbarungen erfolgen, in denen konkrete Sicherheitsanforderungen festgelegt werden. Zudem spielen Zertifizierungen eine wichtige Rolle, um die Einhaltung definierter Standards nachzuweisen.

Das [TISAX®-Label](#) ist seit mehreren Jahren ein wesentliches Erfordernis für Zulieferer in der Automobilbranche. Ziel dieses Standards ist es unter anderem, zu verhindern, dass böswillige Akteure durch sogenannte Supply-Chain-Angriffe Zugriff auf sensible Informationen – etwa Prototypen oder Kundendaten – großer Automobilhersteller erlangen, indem sie die Informationssysteme von Zulieferern angreifen.

Derartige Angriffe können erhebliche wirtschaftliche und reputative Schäden verursachen. Ein standardisiertes Informationssicherheitsmanagementsystem trägt dazu bei, solche Risiken systematisch zu reduzieren.

3. Sicherheitsvorfälle melden und angemessen behandeln

Unternehmen, die als Betreiber kritischer Infrastruktur in den Anwendungsbereich der NIS2 fallen, sind verpflichtet, ihre nationale Cybersicherheitsbehörde unverzüglich über erhebliche Störungen, Sicherheitsvorfälle oder Bedrohungen ihrer kritischen Dienstleistungen zu informieren.

Im Rahmen der Umsetzung der NIS-2 ist zudem ein wirksames Sicherheitsprogramm mit klar definierten Richtlinien und Verfahren für den Umgang mit Sicherheitsvorfällen zu implementieren.

Informationssicherheitsmanagementsysteme nach dem Standard ISO 27001 enthalten regelmäßig entsprechende Vorgaben. Diese umfassen insbesondere Prozesse zur schnellen Identifizierung und Behandlung von Sicherheitsvorfällen, zur Aufrechterhaltung des Geschäftsbetriebs während eines Vorfalls sowie zur Wiederherstellung der Systeme nach einem Notfall.

Unternehmen müssen klare Kommunikationswege, Eskalationsmechanismen und Notfallpläne etablieren, um angemessen auf Sicherheitsvorfälle reagieren zu können. Darüber hinaus sind sie –

soweit erforderlich und möglich – verpflichtet, die Empfänger ihrer Dienstleistungen, also ihre Kunden, über relevante Vorfälle zu informieren.

Weitere wichtige Pflichten nach der NIS-2-Richtlinie

Gemäß der NIS-2-Richtlinie müssen Unternehmen weitere zahlreiche Pflichten erfüllen. Die Geschäftsführung betroffener Einrichtungen ist verpflichtet, die Einhaltung dieser Anforderungen gemäß der jeweiligen nationalen Umsetzungsgesetzgebung zu überwachen. Dabei ist zu beachten, dass im Falle von Verstößen unter Umständen eine persönliche Haftung der Geschäftsführung in Betracht kommen kann.

- **Policies**
Unternehmen müssen verbindliche Richtlinien für das Risikomanagement und die Informationssicherheit entwickeln und implementieren. Diese dienen als Handlungsrahmen für den Umgang mit Cybersicherheitsrisiken und stellen sicher, dass geeignete Schutzmaßnahmen systematisch umgesetzt werden.
- **Business Continuity Management**
Betreiber müssen geeignete Maßnahmen im Rahmen des Business Continuity Managements (BCM) ergreifen, um die Aufrechterhaltung kritischer Dienstleistungen auch im Falle eines Cybervorfalles sicherzustellen. Hierzu zählen insbesondere Backup-Strategien, Krisenmanagementstrukturen sowie Wiederanlauf- und Wiederherstellungspläne.
- **Beschaffung und Einkauf**
Sicherheitsaspekte sind auch bei der Beschaffung von Informations- und Netzwerksystemen zu berücksichtigen. Unternehmen müssen die Sicherheitsmerkmale und -standards der erworbenen Produkte und Dienstleistungen prüfen, um sicherzustellen, dass diese den geltenden Sicherheitsanforderungen entsprechen.
- **Effektivität und Wirksamkeitskontrolle**
Unternehmen müssen Maßnahmen zur Messung der Effektivität ihrer Cyber-Security- und Risikomanagement-Maßnahmen implementieren. Dies ermöglicht ihnen, die Wirksamkeit ihrer Sicherheitsmaßnahmen zu bewerten und bei Bedarf Anpassungen vorzunehmen.
- **Schulung und Sensibilisierung („Cybersecurity-Hygiene“)**
Die NIS-2 sieht vor, dass Mitarbeitende regelmäßig im Bereich Cybersicherheit geschult werden. Unter dem Begriff „Cybersecurity-Hygiene“ werden grundlegende Verhaltensweisen verstanden, die zur Minimierung von Cyberrisiken beitragen. Hierzu zählen beispielsweise ein sicheres Passwortmanagement, das Erkennen von Phishing-E-Mails sowie der verantwortungsvolle Umgang mit sensiblen Daten und IT-Systemen.
- **Kryptografie**
Unternehmen müssen Vorgaben für den Einsatz von Verschlüsselungstechnologien definieren und diese – soweit technisch und organisatorisch möglich – implementieren. Kryptografische Maßnahmen dienen dem Schutz der Vertraulichkeit und Integrität von Informationen.
- **Personalwesen**
Es sind geeignete Maßnahmen zur Sicherstellung der personellen Sicherheit zu treffen. Hierzu gehören insbesondere Zugangskontrollen, Berechtigungskonzepte sowie die Gewährleistung, dass ausschließlich autorisiertes Personal Zugriff auf sensible Systeme und Daten erhält.
- **Authentifizierung**
Zur Sicherstellung der Vertraulichkeit von Informationen sollten geeignete Authentifizierungsmechanismen eingesetzt werden. Hierzu zählen insbesondere Multi-Faktor-Authentifizierung sowie – sofern sinnvoll – Single-Sign-On-Lösungen zur Absicherung von Zugängen.

- **Kommunikation**

Die Verschlüsselung von Sprach-, Video- und Textkommunikation stellt eine wesentliche Maßnahme dar, um die Vertraulichkeit und Integrität von Kommunikationsinhalten zu gewährleisten.

- **Notfall-Kommunikation**

Unternehmen sollten darüber hinaus gesicherte Notfallkommunikationssysteme implementieren, um im Krisenfall eine verlässliche interne und externe Kommunikation sicherzustellen.

NIS-2 und europäische Zusammenarbeit

Ein zentrales Element der NIS-2 ist die verstärkte Zusammenarbeit der Mitgliedstaaten im Bereich der Cybersicherheit. Der Richtliniengeber trägt damit der grenzüberschreitenden Natur von Cyberbedrohungen Rechnung und fordert eine koordinierte europäische Reaktion auf entsprechende Gefahrenlagen.

Die Bedeutung der NIS-2 ist angesichts zunehmender Cyberbedrohungen erheblich. Unternehmen und Organisationen sind gehalten, geeignete Maßnahmen zu ergreifen, um ihre Netzwerke und Informationen nachhaltig zu schützen.

Die Einhaltung der NIS2-Richtlinie wird zu einer Priorität für Unternehmen in ganz Europa, da sie sicherstellen müssen, dass ihre Sicherheitsvorkehrungen den strengen Anforderungen entsprechen.

Umsetzung und Ausblick

Die NIS-2-Richtlinie wurde am 14. Dezember 2022 verabschiedet und ist von den Mitgliedstaaten in nationales Recht umzusetzen. Mit Inkrafttreten der nationalen Umsetzungsvorschriften werden die Anforderungen verbindlich.

Die Implementierung und Überwachung der NIS-2-Standards stellt für viele Unternehmen eine komplexe organisatorische und technische Herausforderung dar, die erhebliche personelle und finanzielle Ressourcen erfordern kann.

Jährlich erfolgt eine Auditierung unseres Qualitätsmanagementsystems einschließlich ESG- und KRITIS-Elementen durch einen qualifizierten Auditor der akkreditierten Gesellschaft Bureau Veritas. Zusätzlich haben wir den Code of Conduct des VDB, VDMA und ZVEI bestätigt.

Gemäß § 289b Abs. 1 HGB ist die SBF-Gruppe nicht verpflichtet, ein KRITIS-Statement abzugeben. Weder handelt es sich bei den Unternehmen der SBF-Gruppe um große Kapitalgesellschaften gemäß § 267 Abs. 3 HGB, noch beschäftigt die SBF-Gruppe mehr als 500 Mitarbeiter.

Leipzig, 30.01.2026



Robert Stöcklinger

CEO

SBF AG

Zaucheweg 4, 04316 Leipzig, Germany

www.sbf-ag.com