orka Newsletter | Datenschutz, IT & Outsourcing | Energierecht

BNetzA: Neue IT-Sicherheitsanforderungen für Betreiber von Energieanlagen

Als Teil eines besonders kritischen Sektors unterliegt die **Energiewirtschaft** verschärften regulatorischen Anforderungen im Bereich der Cybersicherheit. Ziel der regulatorischen Anforderungen ist es, Risiken für die IT-Systeme, die für den Betrieb oder die Erbringung energiewirtschaftlicher Dienste eingesetzt werden, wirksam zu beherrschen.

Betreiber von Energieanlagen – also Anlagen zur Erzeugung, Speicherung, Fortleitung oder Abgabe von Energie, soweit sie nicht lediglich der Übertragung von Signalen dienen – unterliegen gesetzlichen Anforderungen, die sie zur **Gewährleistung eines hohen IT-Sicherheitsniveaus ihrer Energieanlagen** verpflichten.

Energieanlagen gelten unter bestimmten Voraussetzungen als **„Kritische Infrastrukturen" (KRITIS)**. In dieser Eigenschaft können Energieanlagen unterschiedlichen gesetzlichen Anforderungen im Bereich der IT-Sicherheit unterfallen.

Sowohl das Gesetz über das Bundesamt für Sicherheit in der Informationstechnik **(BSIG)** als auch das Energiewirtschaftsgesetz **(EnWG)** enthalten spezifische **Pflichten im Kontext der IT-Sicherheit** – etwa zu der Umsetzung angemessener technischer und organisatorischer IT-Sicherheitsmaßnahmen oder zur Meldung erheblicher Störungen an die zuständigen Behörden.

Anfang Mai 2025 kündigte die **Bundesnetzagentur (BNetzA)** eine Überarbeitung der Anforderungen an die Cybersicherheit im Energiebereich an. In einer Pressemitteilung vom 7. Mai 2025 veröffentlichte die BNetzA die **Entwürfe aktualisierter IT-Sicherheitskataloge**, u.a. für die Betreiber von Energieanlagen.

Zudem wurde ein **neuer Gesetzesentwurf zur Umsetzung der europäischen NIS-2-Richtlinie** veröffentlicht, der unter bestimmten Voraussetzungen auch auf Betreiber von Energieanlagen Anwendung finden.

IT-Sicherheitsanforderungen für Energieanlagen

Besondere regulatorischen IT-Sicherheitsanforderungen können sich für die Betreiber von Energieanlagen aktuell aus zwei zentralen Gesetzen ergeben: Dem EnWG und dem BSIG. Beide setzen voraus, dass die betreffende **Energieanlage als „Kritische Infrastruktur" (KRITIS)** eingestuft wird.

Die Voraussetzungen hierfür ergeben sich aus dem BSIG und der zugehörigen Rechtsverordnung – der **KRITIS-Verordnung**. Die KRITIS-Verordnung definiert **branchenspezifische Schwellenwerte** für unterschiedliche Anlagenkategorien. Sofern eine Anlage den maßgeblichen Schwellenwert erreicht oder überschreitet, gilt sie als „Kritische Infrastruktur".

Beispielsweise gelten **Erzeugungsanlagen im Bereich der Stromversorgung** als KRITIS, wenn ihre installierte Nettonennleistung mindestens 104 MW beträgt. Für bestimmte Erzeugungsanlagen gelten gemäß der KRITIS-Verordnung geringere Schwellenwerte.

Für Energieanlagen, die die jeweiligen Schwellenwerte der KRITIS-Verordnung erreichen bzw. überschreiten, gelten **besondere IT-Sicherheitsanforderungen**. Betreiber von KRITIS-Energieanlagen werden durch das BSIG verpflichtet, angemessene organisatorische und technische Maßnahmen zu ergreifen, um Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer IT-Systeme, Komponenten oder Prozesse zu vermeiden, sofern diese für die Funktionsfähigkeit der jeweiligen Energieanlage maßgeblich sind (§ 8a BSIG).

Vorrangig haben Betreiber von Energieanlagen, die als KRITIS eingestuft sind, jedoch die **speziellen Anforderungen des § 11 EnWG** zu beachten.

Gemäß § 11 Abs. 1b EnWG müssen Betreiber von Energieanlagen, die als KRITIS eingestuft und an ein Energieversorgungsnetz angeschlossen sind, durch geeignete technische und organisatorische Maßnahmen einen **angemessenen Schutz ihrer IT-Systeme gegen Bedrohungen sicherstellen**, soweit die IT-Systeme für einen sicheren Anlagenbetrieb notwendig sind. Hierzu gehört insbesondere der Einsatz

von Systemen zur Angriffserkennung, die kontinuierlich Bedrohungen identifizieren und verhindern können.

In diesem Zusammenhang veröffentlichte die **BNetzA** zuletzt im Jahr 2018 einen **Katalog von Sicherheitsanforderungen**, der sowohl konkrete Sicherheitsmaßnahmen als auch Regelungen zur regelmäßigen Überprüfung ihrer Umsetzung enthielt.

Betreiber von Energieanlagen, die die Anforderungen des IT-Sicherheitskatalogs einhalten, gewährleisten damit ein angemessenes Sicherheitsniveau und erfüllen die gesetzlichen Anforderungen gemäß § 11 Abs. 1b EnWG.

In ihrer Pressemitteilung vom 7. Mai 2025 kündigte die BNetzA nun eine **Aktualisierung des IT-Sicherheitskatalogs für Energieanlagenbetreiber** an. Parallel dazu soll auch der Sicherheitskatalog für Strom- und Gasnetzbetreiber überarbeitet werden.

Ziel der Überarbeitung der IT-Sicherheitskataloge ist es nach Angaben der BNetzA, auf die **zunehmende Digitalisierung im Energiesektor** sowie den Wandel der Bedrohungslage zu reagieren. Zu diesem Zweck sollen die IT-Sicherheitskataloge weitgehend vereinheitlicht und noch enger an dem prozessorientierten Ansatz der ISO/IEC 27001 angelehnt werden.

Mit den neuen IT-Sicherheitskatalogen möchte die BNetzA u.a. einheitliche Begriffsdefinitionen für alle Betreiber schaffen. Zudem solle zwischen allgemeinen **Maßnahmen zur Cybersicherheit sowie zur Aufrechterhaltung der Betriebsfähigkeit** (Business Continuity Management – BCM) sowie spezifischen, durch Zertifizierung nachzuweisenden Sicherheitsanforderungen differenziert werden, so die BNetzA in ihrer Pressemitteilung.

Nach Auffassung der BNetzA werden durch die neue **Prozessorientierung** effektivere und effizientere Risikoanalysen sowie eine noch stärkere Verzahnung von Informationssicherheit und BCM ermöglicht.

Kontaktstelle & Meldepflicht

Neben der Pflicht zur Umsetzung angemessener Sicherheitsmaßnahmen sind Betreiber von KRITIS-Energieanlagen grundsätzlich verpflichtet, **Störungen ihrer IT-Systeme, Komponenten oder Prozesse** in Bezug auf deren Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit **an**

das Bundesamt für Sicherheit in der Informationstechnik (BSI) zu melden, sofern diese zu Ausfällen oder erheblichen Beeinträchtigungen der Energieanlage geführt haben oder führen könnten.

Das EnWG bestimmt dabei spezifische Anforderungen an Form und Inhalt solcher Störungsmeldungen. Diese müssen über eine benannte **Kontaktstelle des Betreibers** an das BSI übermittelt werden (§ 11 Abs. 1c EnWG). Betreiber von KRITIS-Energieanlagen sind zudem verpflichtet, spätestens bis zum 1. April eines jeden Jahres, die von ihnen betriebene Anlage beim BSI zu **registrieren** und dem BSI eine Kontaktstelle zu benennen, die für Rückfragen zur Verfügung steht. Das BSI übermittelt die Registrierungen einschließlich der damit verbundenen Kontaktdaten an die BNetzA weiter.

Neue Anforderungen durch die NIS-2-Richtlinie

Die Rechtslage im Bereich der Cybersicherheit unterliegt einer kontinuierlichen Weiterentwicklung. Mit Datum vom 26.05.2025 wurde ein **neuer Gesetzesentwurf zur Umsetzung der NIS-2-Richtlinie** veröffentlicht, der auch für die Betreiber von Energieanlagen relevant ist.

Ziel der NIS-2-Richtlinie ist es, die Cybersicherheit in der EU zu stärken und einheitliche **Sicherheitsstandards für IT-Systeme, insbesondere in kritischen Infrastrukturen** und wesentlichen Diensten, zu schaffen.

Die NIS-2-Richtlinie hätte ursprünglich bereits zum 17. Oktober 2024 in deutsches Recht umgesetzt werden müssen. Aufgrund der Neuwahlen zum Deutschen Bundestag konnte der Gesetzesentwurf

der alten Bundesregierung jedoch nicht mehr rechtzeitig verabschiedet werden.

Der **Anwendungsbereich der NIS-2-Richtlinie** erstreckt sich grundsätzlich auf öffentliche und private Stellen, die bestimmte Einrichtungsarten betreiben, als mittlere Unternehmen gelten und ihre Dienste in der EU erbringen bzw. ihre Tätigkeiten in der EU ausüben.

Die **Einstufung als „mittleres Unternehmen“** setzt in der Regel mindestens 50 Beschäftigte oder einen Jahresumsatz bzw. eine Jahresbilanzsumme von über 10 Mio. EUR voraus.

Davon abweichend gilt die **NIS-2-Richtlinie für KRITIS-Betreiber** unabhängig von der Unternehmensgröße oder Finanzkennzahlen. Es ist zu erwarten, dass der deutsche Gesetzgeber die dafür maßgebliche KRITIS-Verordnung im Zuge der Umsetzung der NIS-2-Richtlinie ebenfalls anpassen wird.

Betreiber von Energieanlagen können aus verschiedenen Gründen in den Anwendungsbereich der NIS-2-Richtlinie fallen. Beispielsweise gilt die NIS-2-Richtlinie für Betreiber von Energieanlagen, die als **Elektrizitätsunternehmen** im Sinne der Elektrizitätsbinnenmarkt-Richtlinie (RL

(EU) 2019/944) einzustufen sind und die **Funktion der „Versorgung" wahrnehmen**, d.h. Elektrizität an Kunden verkaufen, einschließlich im Wege des Weiterverkaufs.

Unternehmen, die in den Anwendungsbereich der NIS-2-Richtlinie fallen, müssen – vergleichbar mit den dargestellten Anforderungen aus § 11 Abs. 1b EnWG – geeignete technische, operative und organisatorische **Risikomanagementmaßnahmen ergreifen, um Risiken für ihre IT-Systeme zu beherrschen** und Auswirkungen von Sicherheitsvorfällen zu verhindern oder möglichst gering zu halten.

Außerdem statuiert die NIS-2-Richtlinie **verschärfte Meldepflichten**: insbesondere müssen erhebliche Sicherheitsvorfälle **innerhalb von 24 Stunden** nach Kenntniserlangung an die zuständige Behörde gemeldet werden. Die Einhaltung dieser Anforderungen setzt die Implementierung eines geeigneten unternehmensinternen Meldesystems voraus.

Besondere Anforderungen ergeben sich aus der NIS-2-Richtlinie für die **Leitungsorgane verpflichteter Unternehmen.** Geschäftsführungen und vergleichbare Leitungsorgane werden zukünftig unmittelbar verpflichtet, die ergriffenen **Risikomanagementmaßnahmen im Bereich der Cybersicherheit zu billigen und ihre Umsetzung zu überwachen**.

Zudem sieht die NIS-2-Richtlinie vor, dass Leistungsorgane durch die Unternehmen für Verstöße verantwortlich gemacht werden. Leitungsorgane werden zukünftig persönlich starker in die Pflicht genommen, womit **erhöhte Haftungsrisiken** einhergehen könnten.

Für Unternehmen mit Sitz oder Tätigkeit in Deutschland entstehen erst dann konkrete rechtliche Pflichten, wenn die NIS-2-Richtlinie in nationales Recht formal umgesetzt worden ist. Bis zum **Inkrafttreten eines deutschen Umsetzungsgesetzes** gelten die bisherigen Vorschriften – insbesondere § 11 EnWG – fort.

Ihre Ansprechpartner

Dr. Ulla Kelp, LL.M.
Rechtsanwältin, Partnerin
Datenschutz, IT & Outsourcing

T +49 211 600 35-176
ulla.kelp@orka.law

Dr. Philipp Mels
Rechtsanwalt, Partner
Datenschutz, IT & Outsourcing

T +49 211 600 35-180
philipp.mels@orka.law

Dr. Michael Grobe-Einsler
Rechtsanwalt, Salary Partner
Datenschutz, IT & Outsourcing

T +49 211 600 35-450
michael.grobe-einsler@orka.law

Felix Meurer
Rechtsanwalt, Salary Partner
Datenschutz, IT & Outsourcing

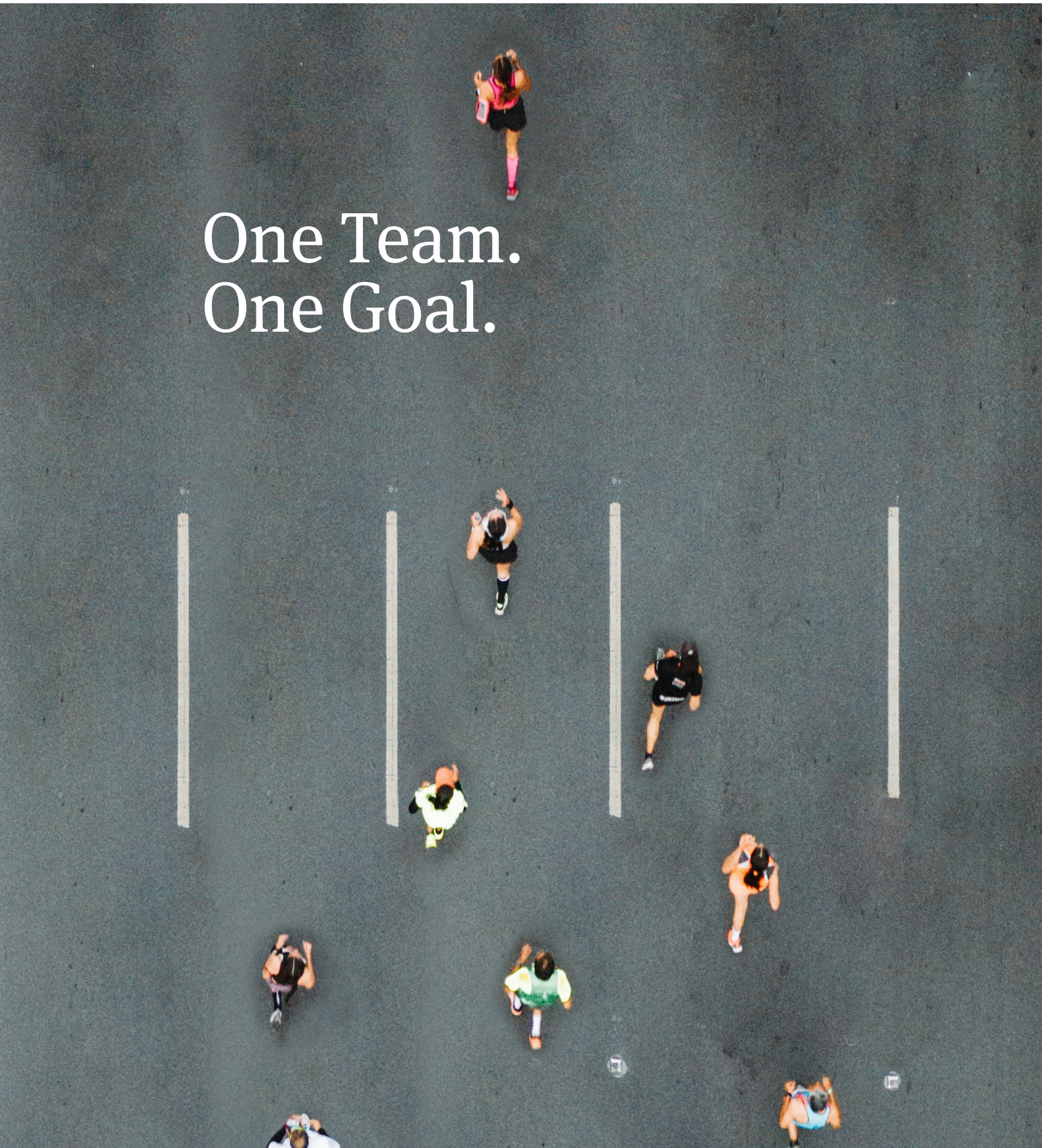
T +49 30 50 93 20-117
felix.meurer@orka.law

Margarete von Oppen
Rechtsanwältin, Partnerin
Energierecht

T +49 30 50 93 20-147
margarete.vonoppen@orka.law

Dr. Dominika Stachurski
Rechtsanwaltin, Salary Partnerin
Energierecht

T +49 30 50 93 20-120
dominika.stachurski@orka.law


One Team.
One Goal.