

NIS2: So müssen sich Energieversorger vor Cyberangriffen schützen

Im Juli 2025 meldete der Militärische Abschirmdienst Medienberichten zufolge einen deutlichen Anstieg von Ausspähversuchen und Störmaßnahmen durch den russischen Geheimdienst. Dass auch die deutsche Energieinfrastruktur Ziel von Sabotageaktionen sein könnte, wird immer realistischer.

Mehrere deutsche Stadtwerke und Energieversorger wurden bereits Opfer gezielter Cyberangriffe. Hacker spähten sensible Daten aus, verschlüsselten Systeme mit Ransomware oder legten zeitweise interne IT-Strukturen lahm. Die Fälle machen deutlich, wie verwundbar unsere Energieversorgung ist. Die NIS-2-Richtlinie der EU zwingt Betreiber kritischer Infrastrukturen künftig dazu, ihre Schutzmaßnahmen gegen Cyberangriffe deutlich zu erhöhen. Die EU hatte die erste Richtlinie zur Regulierung der Cybersicherheit bereits im Juli 2016 verabschiedet. Mit der Richtlinie (EU) 2022/2555 über Maßnahmen für ein hohes gemeinsames [Cybersicherheitsniveau](#) in der Union (Network and Information Security Directive 2 – [NIS 2](#)) erweiterte sie 2022 den Anwendungsbereich, verschärfte die Sicherheits- und Meldepflichten und führte erstmals Sanktionen ein. Seit dem 24. Juni 2025 liegt der [Referentenentwurf des deutschen Gesetzes zur Umsetzung der NIS-2-Richtlinie](#) vor. Parallel dazu wird auch die Bundesnetzagentur tätig und konsultiert im Hinblick auf die konkreten Ausgestaltungen der KRITIS in der Energiewirtschaft einen neuen [IT-Sicherheitskatlog](#).

Im Energiesektor gibt es noch einige Schwachstellen

Angriffspunkte für Cyberangriffe gibt es im Energiesektor noch einige. Viele Leitwarten von Netzbetreibern sind nicht rund um die Uhr besetzt; Mitarbeitende schalten sich in den Randzeiten remote in die Systeme. Das eröffnet auch Hackern Zugriffsmöglichkeiten.

Auch die Gebäude der Energieversorger sind nicht immer zutrittssicher und bieten Kriminellen somit Zutritt in das Haus-(W-)LAN. Umspannwerke und Trafostation stehen teilweise auf frei zugänglichen Feldern bzw. im öffentlichen Straßenraum. In den Bereichen der Gasversorgung sowie Wasser und Abwasser sieht es nicht besser aus: Pump- und Verteilerstationen sind oftmals rein IT-gesteuert über Fernwirktechnik.

Schon die NIS-2-Richtlinie schreibt nicht nur technische, sondern auch organisatorische Maßnahmen vor

Die NIS-2-Richtlinie erfasst eine Vielzahl kritischer und wichtiger Sektoren, neben der Energieversorgung unter anderem das Gesundheitswesen, den Transport, die digitale Infrastruktur sowie zentrale Bereiche der öffentlichen Verwaltung. Erfasst sind Unternehmen und Einrichtungen, deren Ausfall erhebliche Auswirkungen auf das öffentliche Leben, die Wirtschaft oder die Sicherheit haben könnte.

Die Richtlinie schreibt nicht nur technische Vorkehrungen vor, sondern verpflichtet Unternehmen auch zu organisatorischen Maßnahmen zum Schutz ihrer IT-Infrastruktur. Dazu gehört vor allem ein Risikomanagement. Sicherheitsvorfälle müssen gemeldet werden. Zusätzlich müssen andere von dem Vorfall betroffene Einrichtungen informiert werden.

NIS 2 regelt auch: Zur Umsetzung und Überwachung sind die Mitglieder der Geschäftsleitung persönlich

verpflichtet.

Als Sektoren mit hoher Kritikalität beschreibt der Anhang 1 zur NIS2-Richtlinie die Energiewirtschaft. Dies bedeutet unter anderem, dass Einrichtungen in diesem Sektor viele Mindestanforderungen an IT-Sicherheit vorhalten müssen und Betreiber kritischer Infrastruktur zudem zusätzliche Nachweispflichten treffen.

Entwurf des NIS-2-Umsetzungsgesetz enthält auch Ergänzungen im Energiewirtschaftsgesetz (EnWG)

Als EU-Richtlinie muss diese in nationales Recht umgesetzt werden. Einen neuen [Entwurf des NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz](#) (NIS2UmsuCG) hat das Bundesinnenministerium am 23. Juni 2025 vorgelegt. Das [NIS2UmsuCG](#) soll mit Blick auf die Energiewirtschaft vor allem das BSI-Gesetz und das EnWG ändern. Hier ist für den Energiesektor insb. der neue, sehr umfangreiche § 5c EnWG-E relevant. Dort ist auch der IT-Sicherheitskatalog der Bundesnetzagentur gesetzlich verankert, dessen aktuelle Fassung bis dato schon über § 11 Abs. 1a und 1b EnWG von Betreibern umzusetzen ist. Zukünftig verpflichtet er Netzbetreiber und sonstige Betreiber kritischer Energieanlagen zu einem systematischen Risikomanagement für ihre IT-Systeme sowie zum Einsatz von Angriffserkennungssystemen. Sicherheitsvorfälle müssen die Betreiber in der Regel innerhalb von 24 Stunden melden. Im Einzelnen:

- **Angemessener Schutz:** Betreiber von Energieversorgungsnetzen und -anlagen sollen einen angemessenen Schutz gegen Bedrohungen für Telekommunikations- und elektronische Datenverarbeitungssysteme gewährleisten müssen, die für den sicheren Betrieb notwendig sind.
- **Dokumentationspflicht:** Betreiber sollen die Einhaltung der Anforderungen des IT-Sicherheitskatalogs dokumentieren und der Bundesnetzagentur vorlegen müssen. Bei Sicherheitsmängeln kann die Bundesnetzagentur Maßnahmen zur Mängelbeseitigung verlangen.
- **Meldung von Sicherheitsvorfällen:** Betreiber sollen erhebliche Sicherheitsvorfälle innerhalb von 24 bzw. 72 Stunden an eine gemeinsame Meldestelle melden müssen. Die Meldungen sollen detaillierte Informationen über den Vorfall und die ergriffenen Maßnahmen enthalten.
- **Schulungen und Haftung:** Geschäftsleitungen der Betreiber sollen regelmäßig an Schulungen teilnehmen, um ihre Kenntnisse im Bereich der IT-Sicherheit zu verbessern. Sie haften für Schäden, die durch die Verletzung ihrer Pflichten entstehen.
- **Kritische Komponenten und Funktionen:** Die Bundesnetzagentur soll im IT-Sicherheitskatalog festlegen, welche Komponenten und Funktionen als kritisch gelten und welche Sicherheitsanforderungen für deren Betrieb erfüllt werden müssen.

Der IT-Sicherheitskatalog: Neue Festlegung wahrscheinlich noch im Jahr 2025

Neben der durch das NIS2UmsuCG bedingten Ergänzung des EnWG wird darüber hinaus auch auf untergesetzlicher Ebene der IT-Sicherheitskatalog angepasst. Die Bundesnetzagentur (BNetzA) und das Bundesamt für Sicherheit in der Informationstechnik (BSI) haben den [IT-Sicherheitskatalog 2025](#) nach Durchführung einer Konsultation der Marktteilnehmer um neue kritische Funktionen im Energiesektor ergänzt und in ihrer Festlegung auch schon NIS 2 berücksichtigt.

Entsprechend der Vermutungsregelungen in § 11 Abs 1a) und 1b) EnWG liegt ein angemessener Schutz des Betriebs eines Energieversorgungsnetzes bzw. des Betriebs einer Energieanlage vor, wenn dieser Katalog der Sicherheitsanforderungen eingehalten und dies vom Betreiber dokumentiert worden ist. Die neuen Festlegungen

verpflichten daher nicht nur Betreiber von Energieversorgungsnetzen, sondern auch weitere Markttrollen, die zur kritischen Infrastruktur zählen, wie zum Beispiel TK-/EDV-Systeme, Offshore-Windenergieanlagen und sonstige KRITIS-Energieanlagen.

Betreiber von Strom- und Gasnetzen sowie von Energieanlagen sind künftig verpflichtet, dem Bundesinnenministerium anzeigen, wenn sie als kritisch festgelegte IT-Komponenten installieren. Das BMI bewertet dann die Sicherheitsrisiken und kann den Einsatz bestimmter Komponenten untersagen.

Kritische technische Funktionen im Energiesektor sind unter anderem die Netz- und Systemsteuerung (zum Beispiel Leittechnik, Netzschutz und Maßnahmen wie Redispatch und Frequenzhaltung) sowie deren Fernwartungszugänge und auch jegliche Notfallkommunikation.

Die Festlegung kritischer Funktionen gelten für Übertragungsnetzbetreiber bereits ab dem 25. Dezember 2025. Hier werden die Funktionen der Netz- und Systemsteuerung (Steuerung, Leittechnik und Netzschutz) von HVDC-Verbindungen als kritische Funktionen bestimmt. Bei Betreibern von Offshore-Windenergieanlagen sind sämtliche im IT-Sicherheitskatalog genannten Funktionen als kritisch einzustufen.

Mit Wegfall der Anzeigepflicht nach § 9b Abs. 1 Satz 1 BSIG gelten in einem zweiten Schritt dann auch die im Sicherheitskatalog bezeichneten Funktionen für alle Betreiber von Energieversorgungsnetzen und von Energieanlagen, die durch Rechtsverordnung als kritische Infrastruktur eingestuft sind, als kritisch.

Energieversorger sollten ihre Prozesse jetzt schon anpassen

Die schon beschlossenen und die demnächst anstehenden Verschärfungen der Sicherheitsanforderungen sind insbesondere im Bereich der Netz- und Systemsteuerung und der Netzinfrastruktur bereits spürbar. Sämtliche Markttrollen der Energiewirtschaft können und sollten bereits jetzt damit beginnen, ihre Prozesse und ihre Dokumentation anzupassen, um Haftungsrisiken zu minimieren. Dazu gehört insbesondere die Anpassung von Betriebshandbüchern und internen Richtlinien.

Ansprechpartner:

Dirk-Henning Meier

Tel:

dirkhenningmeier@kpmg-law.com