Future Energy
Lab

STUDIE

Cybersicherheits-Zertifizierungen vernetzter Systeme in der Energiewirtschaft

Herausforderungen durch fragmentierte Nachweisverfahren und regulatorischen Wandel im Kontext integrierter OT-Sicherheit

Ein Projekt der
dena

Impressum

Herausgeber:
Deutsche Energie-Agentur GmbH (dena)
Chausseestraße 128 a
10115 Berlin
Tel.: +49 30 66 777-0
Fax: +49 30 66 777-699
E-Mail: info@dena.de
Internet: www.dena.de, www.future-energy-lab.de

Autoren:
Dr.-Ing. Andreas Kubis, c.con Management Consulting GmbH
Peer Buhre, c.con Management Consulting GmbH
Dr.-Ing. Mathias Uslar, OFFIS – Institut für Informatik

Redaktion:
Jasmin Wagner, dena
Marius Dechand, dena
Friederike Wenderoth, dena

Bitte zitieren als:

Deutsche Energie-Agentur (Hrsg.) (dena, 2025): Cybersicherheits-Zertifizierungen vernetzter Systeme in der Energiewirtschaft. Herausforderungen durch fragmentierte Nachweisverfahren und regulatorischen Wandel im Kontext integrierter OT-Sicherheit, Berlin

Bundesministerium für Wirtschaft und Energie

Die Veröffentlichung dieser Publikation erfolgt im Auftrag des Bundesministeriums für Wirtschaft und Energie. Die Deutsche Energie-Agentur GmbH (dena) unterstützt die Bundesregierung in verschiedenen Projekten zur Umsetzung der energie- und klimapolitischen Ziele im Rahmen der Energiewende.

Executive Summary

Die Energiewirtschaft steht im Zentrum der digitalen Transformation und damit auch im Fokus wachsender Cyberrisiken. Mit **der Vernetzung von Information Technology (IT) und Operational Technology (OT), neuen EU-Vorgaben sowie** einem **fragmentierten Zertifizierungsumfeld** wächst der Druck auf Betreiber, Hersteller und Dienstleister, Cybersicherheit nachzuweisen. Doch was passiert, wenn bestehende Prüfverfahren nicht miteinander kompatibel sind? Diese Studie geht der zentralen Frage nach: **Wie können Sicherheitsnachweise** in einem zunehmend vernetzten Energiesystem strukturell integriert und regulatorisch über Rollen, Systeme und Organisationen hinweg **harmonisiert werden**?

Diese Studie untersucht daher **die aktuelle Situation der Cybersicherheits-Nachweise und -Zertifizierungen** in der Energiewirtschaft unter Berücksichtigung der fortschreitenden Vernetzung von IT- und OT-Systemen. Schwerpunkte sind dabei die strukturellen Herausforderungen bei der Umsetzung regulatorischer Anforderungen. Der Fokus liegt dabei nicht nur auf den **Betreibern Kritischer Infrastrukturen (KRITIS)**, sondern ausdrücklich auch auf den Perspektiven von **Herstellern und IT-Dienstleistern**, die in Systemarchitekturen eingebunden sind.

Zentrales Ergebnis der Untersuchungen ist die Erkenntnis, dass es in Deutschland aktuell **drei weitgehend unabhängig voneinander operierende Prüf- und Zertifizierungssysteme** gibt: erstens das ISMS-Zertifizierungsverfahren nach § 11 EnWG (in der Regel auf Basis von ISO/IEC 27001), zweitens die KRITIS-Nachweisführung nach § 8a BSIG sowie drittens die Technischen Richtlinien (TR) des Bundesamts für Sicherheit in der Informationstechnik (BSI). Diese Verfahren sind in Methodik, Zielrichtung und Tiefe aktuell **nicht aufeinander abgestimmt**. Insbesondere beim Zusammenspiel verschiedener Marktrollen innerhalb integrierter Versorgungsunternehmen entstehen dadurch erhebliche Herausforderungen. Die eigentliche Schwierigkeit besteht demnach **weniger im technischen Unvermögen**, sondern entsteht durch das Nebeneinander **nicht inkongruenter Prüfanforderungen**, wodurch sicherheitsrelevante Übergänge aus dem Blick formaler Audits geraten, sodass die Wirksamkeit bestehender Schutzmaßnahmen systemübergreifend kaum nachweisbar ist.

Die Studie motiviert deutlich, dass sich durch neue europäische Regelwerke wie die NIS2-Richtlinie, den **Cyber Resilience Act (CRA)** sowie **nationale Umsetzungsprojekte** (z. B. KRITIS-Dachgesetz) die Anforderungen deutlich verschärfen und auch Hersteller und IT-Dienstleister in die Pflicht genommen werden. Aus diesen Pflichten werden sich **neue Prüf- und Auditierungsanforderungen** ergeben, etwa für Cloud-Dienste, Embedded Systems, SCADA-Komponenten oder digitale Plattformen, die in bestehende betriebliche Sicherheitsnachweise integriert werden müssen.

Ein zentrales Problem identifiziert die Studie in der **mangelnden strukturellen Integration** von Sicherheitsnachweisen: Risikobewertungen, Audits, Schwachstellenanalysen und Betriebsnachweise werden derzeit vielfach parallel, aber nicht aufeinander bezogen durchgeführt.

Die Realität **hybrider Infrastrukturen in der Energiewirtschaft** ist herausfordernd: Historisch gewachsene OT-Systeme treffen auf moderne, zunehmend auch cloudbasierte IT-Strukturen. Die **funktionale Kopplung dieser Systeme bringt Sicherheitsrisiken** mit sich, die in den heutigen Prüfverfahren unzureichend systematisch berücksichtigt werden. Die etablierten Nachweisformate basieren meist auf einer klaren Trennung von Rollen, Verantwortlichkeiten und Systemgrenzen, während in der Praxis häufig übergreifende

Funktionen und Zuständigkeiten vorliegen. Sicherheitsmechanismen bleiben im Rahmen isolierter (Teil-)Prüfungen weitgehend unberücksichtigt.

Besonders veranschaulicht wird dies im **Use Case** dieser Studie, in dem anhand eines **fiktiven integrierten Stadtwerks** die **Herausforderungen** sichtbar werden, mit denen viele Versorgungsunternehmen in Deutschland zunehmend konfrontiert sind. Sie bewegen sich in einem komplexen Spannungsfeld aus technischer Heterogenität, fragmentierten Zuständigkeiten, wachsender regulatorischer Komplexität und Abhängigkeiten von Dritten. **Klassische Audit- und Zertifizierungsverfahren greifen dabei oft zu kurz**, da sie isolierte Teilbereiche prüfen, ohne deren Wechselwirkungen systematisch zu erfassen.

Eine weitere Herausforderung liegt darin, dass strategische Leitlinien meist **keine konkreten Umsetzungsschritte** vorgeben. Zwar beschreiben sie angestrebte Zielzustände, lassen jedoch offen, wie diese in der Praxis erreicht werden können.

Die Studie plädiert daher für eine **systemische Weiterentwicklung der Prüfarchitektur**. Vorgeschlagen wird ein integrierter (Referenz-)Ansatz, der nicht nur funktionale Übergänge zwischen Systemen berücksichtigt, sondern auch die Anerkennung einmal durchgeführter Prüfungen in unterschiedlichen Kontexten ermöglicht. Mit dieser modularen Wiederverwendung geprüfter Elemente können Mehrfachprüfungen vermieden werden. Bei der Umsetzung sollte berücksichtigt werden, konkrete Schritte zur praktischen Umsetzung mit aufzuführen.

Zusammenfassend empfiehlt die Studie die **Entwicklung eines integrierten, modularen Prüfökosystems**, das vorhandene Nachweisverfahren miteinander verzahnt, anwendungsbezogen erweitert und zukünftige regulatorische Anforderungen, insbesondere aus der EU, antizipiert.

Abschließend hebt die Studie hervor, dass die Entwicklung solcher vernetzten Prüfstrukturen auch auf eine **stärkere Zusammenarbeit in der Energiebranche** angewiesen ist, etwa in Form der gemeinsamen Entwicklung von Standards, Pilotprojekte oder sektorübergreifender Resilienzmodelle.

Zentrale Empfehlungen der Studie

Die Studie benennt vier wesentliche Gestaltungsbedarfe für ein zukunftsfähiges Prüfökosystem in der Energiewirtschaft:

1. **Prüfarchitektur modular und anschlussfähig gestalten**
   Nachweisverfahren wie nach § 11 EnWG, § 8a BSIG und BSI-TR sollen besser aufeinander abgestimmt und in einem modularen System zusammengeführt werden. Standardisierte Prüfelemente sollen mehrfach verwendbar sein, zum Beispiel für unterschiedliche Rollen. Einheitliche Bewertungskategorien erhöhen die Vergleichbarkeit und Effizienz.
2. **Systemübergänge und Schnittstellen gezielt prüfen**
   Technisch kritische Übergänge zwischen IT und OT müssen systematisch erfasst und in die Prüfplanung integriert werden. Auch Sicherheitsfunktionen, die sich aus dem Zusammenspiel mehrerer Systeme ergeben (z. B. Notfallmanagement), sollen explizit geprüft werden.
3. **EU-Regulierung aktiv einbeziehen**
   Unternehmen sollten sich frühzeitig mit kommenden Anforderungen aus NIS2, dem Cyber Resilience Act und dem EU-Zertifizierungsrahmen (z. B. EUCC/EUCS) befassen. Ziel ist es, bestehende ISMS- und Auditstrukturen anschlussfähig zu halten und spätere Doppelarbeit zu vermeiden.

4. **Zusammenarbeit und Referenzlösungen fördern**
   Sektorübergreifende Standards und Referenzmodelle für Resilienz sollen helfen, Prüfverfahren zu vereinheitlichen und Nachweise wiederverwendbar zu machen. Pilotprojekte, Branchendialoge und die Beteiligung an Normungsgremien sind hierfür wichtige Hebel.

Die Studie identifiziert zentrale Handlungsbedarfe in Bezug auf Regulierung, Zertifizierung, IT-/OT-Governance und Resilienz, verteilt auf verschiedene Verantwortungsebenen:

- Politik und Aufsichtsbehörden (z. B. BSI, BNetzA, BMWE): Gefordert sind verbindliche Qualifikationsstandards, anschlussfähige Prüfverfahren sowie eine kohärente Umsetzung europäischer Vorgaben.
- Branchenplattformen und Fachverbände: Entwickeln methodische Grundlagen, Prüfelement-Bausteine und sektorspezifische Umsetzungshilfen.
- Kommunale Unternehmen und Stadtwerke: Können operative Maßnahmen zur Segmentierung ihrer Systemen in getrennte Bereiche sowie zum Schnittstellen- und Dienstleistermanagement umsetzen, auch unterhalb formaler KRITIS-Schwellen.
- EU-Institutionen (z. B. ENISA): Gestalten Zertifizierungs- und Registersysteme, die Fragmentierungen überwinden und sektorübergreifende Vergleichbarkeit schaffen.

Eine vollständige Übersicht über die empfohlenen Maßnahmen und ihre Adressaten findet sich in Anhang B dieser Studie.

Inhalt

1 Einleitung

Die Digitalisierung der Energiewirtschaft führt zu einer wachsenden Verzahnung von Systemen der Information Technology (IT) und der Operational Technology (OT). Damit steigen die Anforderungen an die Cybersicherheit insbesondere für Betreiber Kritischer Infrastrukturen (KRITIS), die für eine stabile und resiliente Energieversorgung verantwortlich sind.

Zertifizierungen gewinnen in diesem Kontext an Relevanz: Sie schaffen Vertrauen, dokumentieren die Umsetzung gesetzlicher Sicherheitsanforderungen und gelten als formaler Nachweis gegenüber Aufsichtsbehörden wie dem Bundesamt für Sicherheit in der Informationstechnik (BSI) oder der Bundesnetzagentur (BNetzA). Auch wenn viele Gesetze keine explizite Zertifizierungspflicht beinhalten, fordern sie doch Schutzmaßnahmen nach dem „Stand der Technik“. Zertifizierungen machen diese Anforderungen transparent und überprüfbar.

Besondere Brisanz erhält das Thema durch ausgelagerte IT-Strukturen. Dienstleister, die im Auftrag von KRITIS-Betreibern tätig sind, etwa für Hosting, Fernwartung oder Softwarepflege, geraten zunehmend in den Fokus regulatorischer Aufsicht. Gleiches gilt für Hersteller sicherheitskritischer Komponenten. Die europäische Regulierung verfolgt insbesondere mit der NIS2-Richtlinie und dem geplanten Cyber Resilience Act (CRA) das Ziel, einheitliche Anforderungen und Zertifizierungspflichten für digitale Produkte und Dienstleistungen zu etablieren.

Zentrale Fragestellung dieser Studie

Welche konkreten Pflichten zur IT- und OT-Sicherheit gelten für Betreiber, Hersteller und Dienstleister im Energiesektor und wie lassen sie sich systematisch erfassen, abgrenzen und einordnen?

Als Branchenplattform möchten wir mit der Studie Orientierung schaffen, Handlungspflichten strukturieren und Wege aufzeigen, wie sich bestehende Nachweisverfahren harmonisieren lassen in einem Umfeld, das durch technische Komplexität und regulatorische Dynamik geprägt ist.

Die Studie ist wie folgt gegliedert:

- Kapitel 2 analysiert die geltenden regulatorischen Anforderungen, ordnet sie den relevanten Akteursgruppen zu und beleuchtet bestehende Zertifizierungs- und Nachweisverfahren sowie ihre Überschneidungen und Harmonisierungspotenziale.
- Kapitel 3 zeigt anhand eines realitätsnahen Use Case eines Stadtwerks, das nicht unter die KRITIS-Regulierung fällt, wie verschiedene Prüfregime in der Praxis aufeinandertreffen und welche Herausforderungen sich daraus ergeben.

2 Übersicht über Zertifizierungen im Cybersicherheits-Kontext

Die regulatorischen Anforderungen und die Zertifizierungslandschaft im Bereich der Cybersicherheit sind für die Energiebranche vielschichtig und mitunter schwer überschaubar. Unterschiedliche gesetzliche Vorgaben, Zuständigkeiten und Arten von Prüfverfahren erschweren die Orientierung und stellen Unternehmen vor erhebliche Schwierigkeiten bei der Umsetzung der regulatorischen Vorgaben. Ziel dieses Kapitels ist es daher, eine strukturierte Übersicht über den derzeit geltenden regulatorischen Rahmen zu geben, aufzuzeigen, welche Akteure jeweils betroffen sind, sowie die bestehenden Zertifizierungsverfahren und Zuständigkeiten der relevanten Behörden darzustellen. Darauf aufbauend werden zentrale Herausforderungen identifiziert und Empfehlungen formuliert, wie sich die bestehenden Strukturen gezielt weiterentwickeln und praktikabler gestalten lassen.

Zur besseren Einordnung der in diesem Kapitel beschriebenen Sicherheitsanforderungen und Prüfverfahren ist im Anhang eine Übersicht über die zentralen Normen, Richtlinien und regulatorischen Grundlagen zusammengestellt, auf die im weiteren Verlauf regelmäßig Bezug genommen wird.

2.1 Einordnung des regulatorischen Rahmens

Als KRITIS gelten Organisationen und Einrichtungen mit großer Bedeutung für das Gemeinwesen, deren Ausfall erhebliche Versorgungsengpässe oder Sicherheitsrisiken verursachen würde. Die rechtliche Grundlage dafür bildet das Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz, BSIG), insbesondere § 2 Abs. 10. KRITIS umfasst derzeit neun Sektoren, darunter Energie, Informationstechnologie/Telekommunikation (IT/TK), Gesundheit, Wasser und Transport.

Für den Energiesektor konkretisiert die Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung, BSI-KritisV) diese Einstufung anhand technischer Schwellenwerte, etwa der installierten Erzeugungskapazität, der Netzlänge oder der versorgten Personen (vgl. Tabelle 1). Für Strom gilt: Betreiber gelten als KRITIS-relevant, wenn sie rechnerisch mindestens 500.000 Menschen versorgen. Grundlage ist ein durchschnittlicher Jahresstromverbrauch von 1.815 kWh pro Person.

	Schwellenwert	Bemerkung/Grundlage
Stromerzeugung	104 MW Netto-Nennleistung	Entspricht dem Jahresverbrauch von 500.000 Personen
Steuerung/Bündelung	104 MW Netto-Nennleistung	Erzeugungsanlagen mit Steuerungs- oder Bündelungsfunktion
Schwarzstartfähige Anlagen	0 MW	Jedes schwarzstartfähige Kraftwerk zählt als KRITIS, unabhängig von der Leistung
Primärregelleistung	36 MW präqualifizierte Leistung	Abgeleitet aus der EU-Verordnung 2016/631

Tabelle 1: KRITIS-Schwellenwerte nach Anlagenkategorie (BSI-KritisV; Bundesrepublik Deutschland, 2023)

Betreiber KRITIS-relevanter Infrastrukturen unterliegen den Vorgaben des § 8a BSIG. Er verpflichtet sie dazu, technische und organisatorische Maßnahmen zum Schutz ihrer IT-Systeme zu treffen, um Störungen der

Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit zu verhindern. Maßstab ist jeweils der „Stand der Technik“. Konkret umfasst die Pflicht:

- Risikobasierte Sicherheitskonzepte nach etablierten Normen (z. B. ISO/IEC 27001, B3S, BSI-Grundschutz)
- Einsatz von Angriffserkennungssystemen (§ 8a Abs. 1a BSIG)
- Regelmäßige Nachweisprüfung, mindestens alle zwei Jahre (§ 8a Abs. 3 BSIG)
- Meldepflicht erheblicher IT-Störungen (§ 8b BSIG)

Der Nachweis erfolgt nicht über eine formale Zertifizierung, sondern durch strukturierte Prüfdokumente einer vom BSI anerkannten Prüfstelle. Die Dokumentation besteht aus vier Teilen: (i) PE.M: Beschreibung der Maßnahmen, (ii) PE.R: Risikobewertung, (iii) PE.A: Argumentation zur Angemessenheit, (iv) PE.E: Prüfererklärung. Die Prüfer müssen über die sogenannte Grundsätzliche Anerkennung im Nachweisfahren (BSI-1, 2025) des BSI verfügen; verbindliche ISO-Zertifizierungen oder zentrale Akkreditierungssysteme wie bei der BNetzA bestehen nicht. Die risikobasierte Auslegung erlaubt betriebliche Flexibilität, führt jedoch in der Praxis häufig zu Unsicherheiten, da objektive Maßstäbe oder verpflichtende Kriterien fehlen. Auch deshalb gelten ISO/IEC 27001 oder Branchenspezifische Sicherheitsstandards (B3S) in vielen Fällen als bewährter Referenzrahmen.

Der Nachweis nach § 8a BSIG bezieht sich nicht nur auf unmittelbar kritische Anlagen, sondern auch auf Komponenten, Dienstleistungen und Prozesse, die für ihren sicheren Betrieb wesentlich sind. Dazu zählen:

- Kritische Komponenten (z. B. Steuerungs- oder Kommunikationssysteme), deren Einsatz nach § 9b BSIG nur mit BSI-Zulassung erlaubt ist
- Kritische Dienstleistungen, wie ausgelagerte IT-Wartung, Hosting oder Betriebssupport, sofern sie für die Verfügbarkeit oder Steuerbarkeit der Infrastruktur notwendig sind
- Kritische Funktionen, wie Redispatch, Netzführung oder Wiederanlaufstrategien, auch wenn sie bislang nicht formell gesetzlich definiert sind

Der Begriff „kritische Funktionen“ ist weder im BSIG noch im Energiewirtschaftsgesetz (EnWG) kodifiziert. Zwar enthält das Telekommunikationsgesetz (§ 165 TKG) eine sektorspezifische Definition, sie ist jedoch nicht auf den Energiesektor übertragbar. Die BNetzA hat ein Festlegungsverfahren zur Definition kritischer Funktionen im Energiesektor eingeleitet; eine verbindliche Vorgabe liegt Stand Juli 2025 bislang nicht vor.

Trotz fehlender rechtlicher Verankerung besteht in der Fachpraxis weitgehender Konsens darüber, dass bestimmte systemrelevante Betriebsprozesse, etwa Redispatch oder Wiederanlauf, operativ als sicherheitskritisch zu betrachten sind. Im Rahmen von Audits im Rahmen von § 8a BSIG ist es daher üblich und wird vom BSI erwartet, dass Betreiber diese Funktionen risikobasiert identifizieren und in den Nachweisbereich einbeziehen, sofern sie maßgeblich zur Stabilität Kritischer Infrastrukturen beitragen.

Hinweis zu § 8a BSIG

Die in diesem Abschnitt dargestellten Grundlagen zu § 8a BSIG bilden die Basis für die sektorale und rollenbezogene Vertiefung in den folgenden Kapiteln. Auf eine erneute Darstellung des vollen Prüfrahmens wird dort bewusst verzichtet. Stattdessen wird auf spezifische Umsetzungen und Besonderheiten verwiesen.

Die Verantwortung für die Schutzbedarfsbewertung und die Festlegung des Prüfbereichs liegt beim Betreiber. Die Prüfstelle bewertet im Rahmen des Audits, ob diese Einordnung plausibel und nachvollziehbar erfolgt ist. Eine formale Pflicht zur Prüfung kritischer Funktionen besteht nicht, wohl aber eine regulatorische Erwartung, dass sie im Kontext des sicheren Anlagenbetriebs berücksichtigt werden, auch in Vorbereitung auf künftige EU-weite Vorgaben.

2.2 Rollen, Pflichten und Nachweisrahmen im Energiesektor

Im Energiesektor konkretisiert die BNetzA den gesetzlichen Rahmen durch sektorspezifische Vorgaben. Dazu zählen insbesondere die IT-Sicherheitskataloge für Netzbetreiber (BNetzA, 2015) und Anlagenbetreiber (BNetzA, 2022b), die Anforderungen an Organisation, Technik und Nachweisführung im Bereich der Informationssicherheit festlegen. Die Kataloge konkretisieren entweder energiewirtschaftliche Pflichten nach dem Energiewirtschaftsgesetz (EnWG; Bundesrepublik Deutschland, 2023) oder flankieren die allgemeinen Anforderungen aus dem BSI-Gesetz (BSIG; Bundesrepublik Deutschland, 2023) mit branchenspezifischen Inhalten.

Die IT-Sicherheitskataloge der BNetzA stützen sich auf international anerkannte Normen der ISO/IEC-27000-Reihe, insbesondere ISO/IEC 27001, 27002 und 27019. Die Standards sind inhaltlich aufeinander abgestimmt und gegenseitig referenziert. Während ISO/IEC 27001 die Anforderungen an ein Informationssicherheits-managementsystem (ISMS) beschreibt, konkretisiert ISO/IEC 27002 geeignete Maßnahmen und Kontrollziele. Die ISO/IEC 27019 ergänzt diese um sektorspezifische Anforderungen für den Betrieb industrieller Steuerungs- und Prozessleittechnik in der Energieversorgung. Damit bildet sie eine zentrale normative Grundlage für die Umsetzung der Sicherheitskataloge.

Als ergänzender, praxisorientierter Rahmen hat sich darüber hinaus das Whitepaper des Bundesverbands der Energie- und Wasserwirtschaft (BDEW) „Anforderungen an sichere Steuerungs- und Telekommunikationssysteme“ (BDEW, 2024) etabliert. Es konkretisiert typische Gefährdungsszenarien, Schutzmaßnahmen und Umsetzungsstrategien für Unternehmen im Energiesektor und wird von vielen Marktteilnehmern zur Ausgestaltung ihres ISMS herangezogen. Auch ohne rechtliche Verbindlichkeit gilt es in der Praxis oft als Referenz für den „Stand der Technik“ gemäß § 8a BSIG und § 11 EnWG.

Die sektorspezifischen Vorgaben betreffen verschiedene Akteure, etwa Netzbetreiber, Anlagenbetreiber, Messstellenbetreiber oder Gateway-Administratoren, je nach Rolle, technischer Zuständigkeit und regulatorischer Einordnung.

2.2.1 Betreiber von Energieanlagen

Der Begriff der Energieanlage ist in § 3 Nr. 15 EnWG definiert und umfasst unter anderem Anlagen zur Erzeugung, Speicherung und Abgabe von Energie. Für Betreiber solcher Anlagen, die an ein Energie-versorgungsnetz angeschlossen sind und gemäß BSI-KritisV als KRITIS eingestuft wurden, stellt die BNetzA einen eigenen IT-Sicherheitskatalog für Betreiber von Energieanlagen (BNetzA, 2022b) zur Verfügung.

Der Sicherheitskatalog konkretisiert die Anforderungen aus § 8a BSIG für den Betrieb von Energieanlagen mit KRITIS-Relevanz. Er beschreibt technische und organisatorische Maßnahmen zum Schutz der für den Anlagenbetrieb eingesetzten IT-Systeme, Komponenten und Prozesse. Die Schutzmaßnahmen orientieren sich an den Schutzzielen Verfügbarkeit, Integrität und Vertraulichkeit und werden anhand eines zonenbasierten Schutzklassenmodells strukturiert.

Betreiber sind verpflichtet, die im Katalog beschriebenen Maßnahmen umzusetzen, zu dokumentieren und regelmäßig auf ihre Wirksamkeit zu überprüfen. Zur Nachweisführung können etablierte Sicherheitsstandards wie ISO/IEC 27001 oder anerkannte Branchenspezifische Sicherheitsstandards (B3S) herangezogen werden. Die Anwendung des Sicherheitskatalogs erfolgt im Rahmen der KRITIS-Regulierung und dient als Grundlage für die Erfüllung der Nachweispflichten gegenüber dem BSI.

Netzbetreiber sind vom Anwendungsbereich dieses Sicherheitskatalogs ausdrücklich ausgenommen. Zwar gelten sie gemäß § 3 Nr. 15 EnWG formal ebenfalls als Betreiber von Energieanlagen, jedoch stellt der Sicherheitskatalog in seinem Adressatenkreis klar, dass er nicht für Netzbetreiber gilt. Für sie gelten die Anforderungen des separaten IT-Sicherheitskatalogs nach § 11 Abs. 1a EnWG.

2.2.2 Betreiber von Energieversorgungsnetzen

Betreiber von Strom- und Gasversorgungsnetzen sind gemäß § 11 Abs. 1a EnWG verpflichtet, angemessene Vorkehrungen zum Schutz gegen Bedrohungen für Telekommunikations- und elektronische Datenverarbeitungssysteme zu treffen, die für den sicheren Netzbetrieb erforderlich sind (BNetzA, 2015). Zur Umsetzung hat die BNetzA im Einvernehmen mit dem BSI einen IT-Sicherheitskatalog für den sicheren Betrieb von Energieversorgungsnetzen (BNetzA, 2022b) veröffentlicht.

Der Sicherheitskatalog gilt für alle Netzbetreiber, die IT-Systeme einsetzen, die für die Netzführung, Überwachung oder Steuerung des Netzbetriebs erforderlich sind. Dazu zählen unter anderem Netzleitsysteme, Fernwirktechnik, Netzschutzsysteme sowie Komponenten der Informations- und Kommunikationstechnologie (IKT). Der Katalog ist unabhängig von einer KRITIS-Einstufung anzuwenden und gilt für Netzbetreiber aller Spannungsebenen.

Zentrale Anforderungen sind die Einführung, der Betrieb und die regelmäßige Verbesserung eines ISMS nach Deutschem Institut für Normung (DIN) EN ISO/IEC 27001. Der Betreiber ist verpflichtet, die Umsetzung mittels einer Zertifizierung durch eine akkreditierte Stelle nachzuweisen. Dieses Zertifikat ist auf Anforderung der BNetzA vorzulegen. Alternativ anerkannte Standards wie der IT-Grundschutz des BSI sind nicht vorgesehen.

Sofern keine relevanten informationstechnischen Systeme betrieben werden, ist eine formale Erklärung zur Nichtanwendbarkeit des Sicherheitskatalogs (BNetzA, o.D.) gegenüber der BNetzA einzureichen. Diese Erklärung ist regelmäßig zu aktualisieren und bei Änderungen der Systemlandschaft erneut zu prüfen.

2.2.3 Messstellenbetreiber

Das Messstellenbetriebsgesetz (MsbG) unterscheidet zwischen grundzuständigen (gMSB) und wettbewerblichen Messstellenbetreibern (wMSB). Der gMSB wird gemäß § 4 Abs. 1 MsbG durch den Netzbetreiber bestimmt. Er ist verpflichtet, alle Anschlussnutzer mit modernen Messeinrichtungen bzw. intelligenten Messsystemen auszustatten. Der wMSB kann durch den Anschlussnutzer gewählt werden und muss gemäß § 6 Abs. 2 MsbG technische Gleichwertigkeit sicherstellen.

Für beide gelten beim Einsatz intelligenter Messsysteme dieselben technischen Anforderungen, darunter:

- Datenschutz und Datenintegrität (§ 19 MsbG)
- Mindestanforderungen und Interoperabilität (§§ 20–21)

- Zulassung und Zertifizierung durch das BSI (§§ 22–23)
- Smart-Meter-PKI und Berechtigungskonzepte (§§ 24–28)
- Anwendung von Technischen Richtlinien und Schutzprofilen (§§ 29–31)

Eine formale ISMS-Zertifizierung ist nicht vorgeschrieben. Die Sicherheitspflichten werden durch die zertifizierten Komponenten (v. a. Smart Meter Gateways) abgedeckt.

2.2.4 Gateway-Administrator

Die Administration des Smart Meter Gateway ist eine technisch eigenständige Funktion, die nicht zwingend vom Messstellenbetreiber selbst übernommen werden muss. Der Gateway-Administrator (GWA) ist verantwortlich für die Installation, Konfiguration, Administration, Überwachung und Wartung des Gateways sowie für die Anbindung weiterer technischer Einrichtungen. Er darf ausschließlich vom BSI zertifizierte Gateways verwenden (§ 25 Abs. 1 MsbG) und muss Sicherheitsmängel dem BSI melden. Gemäß § 25 Abs. 4 MsbG ist der GWA verpflichtet,

- ein ISMS zu betreiben,
- eine IT-Sicherheitskonzeption entsprechend den Technischen Richtlinien des BSI zu erstellen und umzusetzen,
- weitere organisatorische und technische Sicherheitsanforderungen einzuhalten,
- regelmäßige Audits durch vom BSI zertifizierte Auditierer durchzuführen und
- die Markt- und Verwendungsüberwachung sowie das Mess- und Eichrecht zu unterstützen.

Die Erfüllung dieser Anforderungen ist gemäß § 25 Abs. 5 MsbG durch ein entsprechendes Zertifikat nachzuweisen, entweder direkt durch das BSI oder durch eine akkreditierte Zertifizierungsstelle nach ISO/IEC 27006-3. Der Auditbericht ist dem BSI vorzulegen. Diese ISMS-Pflicht betrifft ausschließlich die Rolle des GWA, nicht den Messstellenbetreiber als solchen, es sei denn, dieser nimmt die Gateway-Administration selbst wahr.

2.2.5 Aggregatoren

Aggregatoren übernehmen die zentrale Steuerung und Bündelung von Erzeugungs-, Speicher- oder Verbrauchsanlagen, etwa zur Teilnahme an Märkten für Regelenergie, Flexibilität oder Direktvermarktung. Sie gelten gemäß Tabelle 1.1.5 der BSI-KritisV (Bundesrepublik Deutschland, 2023) als KRITIS, wenn sie über Steuerungseinrichtungen verfügen, mit denen sie Anlagen mit einer aggregierten Leistung von mindestens 104 MW zentral technisch steuern oder bündeln. Maßgeblich ist die technische Steuerungsverantwortung, nicht Eigentum oder Bilanzkreiszuordnung.

Bei Erreichen des Schwellenwerts greifen die Anforderungen des § 8a BSIG, insbesondere zur Umsetzung technischer und organisatorischer Sicherheitsmaßnahmen. Grundlage für den Nachweis bildet der Branchenspezifische Sicherheitsstandard (B3S) „Anlagen oder Systeme zur Steuerung / Bündelung elektrischer Leistung“ (BDEW, 2023) des BDEW. Er verpflichtet zur Einführung eines ISMS nach ISO/IEC 27001, ergänzt um Elemente der ISO/IEC 27002 und 27019. Der Geltungsbereich umfasst zentrale

Steuerungssysteme, Kommunikationsschnittstellen, Betriebsprozesse und zugehörige organisatorische Strukturen. Der Nachweis erfolgt über die KRITIS-Prüfung gemäß § 8a Abs. 3 BSIG.

Sofern einzelne Erzeugungs- oder Verbrauchsanlagen, die durch einen Aggregator gebündelt oder angesteuert werden, eigenständig als KRITIS bewertet werden, unterliegen sie nicht dem B3S für Aggregatoren. In solchen Fällen greifen die jeweils einschlägigen sektorspezifischen Regelungen, im Energiesektor insbesondere der IT-Sicherheitskatalog der BNetzA gemäß § 11 Abs. 1b EnWG. Die Verantwortung für die Umsetzung der dort definierten Anforderungen liegt bei den jeweiligen Betreibern der Einzelanlagen.

2.2.6 Hersteller und Dienstleister in der Lieferkette

Hersteller und Dienstleister sind keine unmittelbaren Adressaten der IT-Sicherheitskataloge der BNetzA oder der KRITIS-Vorgaben des BSI. Jedoch bestehen mittelbare Anforderungen, insbesondere:

- § 8a BSIG / § 11 EnWG: Betreiber müssen im Rahmen ihres Sicherheitsnachweises dokumentieren, dass eingesetzte Produkte und Dienstleistungen dem „Stand der Technik“ entsprechen.
- § 9b BSIG: Der Einsatz sogenannter kritischer Komponenten ist nur zulässig, wenn sie zuvor vom BSI zugelassen wurden.

Im Messwesen ergeben sich daraus spezifische Pflichten für Komponentenhersteller und Backend-Betreiber gemäß §§ 22–25 MsbG, etwa im Hinblick auf Zulassung, Zertifizierung und Interoperabilität.

Die Erfüllung dieser Anforderungen muss durch die Betreiber vertraglich abgesichert werden. Eine eigene ISMS-Zertifizierungspflicht für Hersteller oder Dienstleister besteht bislang nicht.

2.2.7 Zusammenfassende Darstellung

Zur Übersicht stellt Tabelle 2 die heutigen regulatorischen Pflichten im Energiesektor dar, gegliedert nach Rollen, zuständigen Behörden, Rechtsgrundlagen und anzuwendenden Standards.

		Pflicht zur Einführung eines ISMS	ISMS-Zertifizierungspflicht	Meldepflicht für Sicherheitsvorfälle	Systeme zur Angriffserkennung	IT-Sicherheitsmaßnahmen nach Stand der Technik
KRITIS	KRITIS-Betreiber - allgemein	ja – explizit	ja – explizit [1]	ja	ja	ja
	Betreiber von Energieanlagen	ja	ja – explizit [1]	ja	ja	ja
	Aggregatoren	ja	implizit [2]	ja	ja	ja
	Betreiber von Energieversorgungsnetzen	ja; ISO 27001	ja – explizit	ja	ja	ja
NICHT-KRITIS	Betreiber - allgemein	nein	nein	nein	nein	nein
	Betreiber von Energieanlagen	nein	nein	nein	nein	nein
	Aggregatoren	nein	nein	nein	nein	nein
	Betreiber von Energieversorgungsnetzen	ja; ISO 27001	ja – explizit	ja	implizit [3]	ja – explizit
	Messstellenbetreiber (gMSB/wMSB)	nein (sofern kein GWA)	nein	nein	nein	ja – explizit
	Smart-Meter-Gateway-Administratoren (GWA)	ja	ja – explizit	ja	implizit [3]	ja – explizit
HERSTELLER	Hersteller - allgemein	nein	nein	nein	nein	nein
	Hersteller von IT/OT für sicherheitskritische Elemente	ja	implizit [3]	nein	implizit [3]	implizit [3]
	Hersteller von Smart-Metering-Infrastruktur	nein, jedoch [4]	nein	nein	nein	implizit [3]
DIENSTLEISTER	Dienstleister - allgemein	nein	nein	nein	nein	nein
	Dienstleister - mit Zugang zu sicherheitskritischen Elemente	ja	implizit [3]	nein	implizit [3]	implizit [3]
	Hosting - allgemein	implizit	nein	nein	nein	nein
	Hosting von sicherheitskritischen Systemen	ja	implizit [3]	nein	implizit [3]	implizit [3]

[1] Durchführung KRITIS-Prüfverfahren nach § 8a BSIG einschließlich Anzeige des Einsatzes kritischer Komponenten
[2] Implizit, als Bestandteil des KRITIS-Prüfverfahrens
[3] Implizit, da i.d.R. Bestandteil vertraglicher Verpflichtungen mit KRITIS-Betreiber zur Erfüllung der IT-Sicherheitsmaßnahmen nach Stand der Technik
[4] Zertifizierung nach Common Criteria (BSI-CC-PP-0073) und BSI TR-03109 erfordern implizit ein ISMS

Tabelle 2: Tabellarische Übersicht über heutige regulatorische Anforderungen sowie Nachweis- und Meldepflichten

2.3 Sicherheitsanforderungen für Hersteller und IT-Dienstleister

Die tabellarische Übersicht über die regulatorischen Anforderungen (Kapitel 2.2.7) zeigt: Die heutigen IT- und OT-Sicherheitsanforderungen im Energiesektor sind stark differenziert, je nach Rolle, Infrastrukturebene und regulatorischer Zuständigkeit. Dabei bestehen nicht nur unterschiedliche Nachweisformate und Zertifizierungsanforderungen, sondern auch komplexe Schnittstellen zwischen den Akteuren, insbesondere entlang der technischen Lieferkette.

In der Praxis stellt diese Vielfalt hohe Anforderungen an Koordination, Verantwortungsabgrenzung und Vertragsgestaltung. Für Betreiber bedeutet das, Sicherheitsanforderungen nicht nur intern umzusetzen, sondern sie auch auf Dienstleister, Hersteller und vorgelagerte Partner zu übertragen, häufig ohne klar definierte formale Rahmenbedingungen. Gleichzeitig existieren Mehrfachanforderungen und ungleiche Prüftiefen, etwa zwischen § 8a BSIG, § 11 EnWG und den Vorgaben des Messstellenbetriebsgesetzes.

Die Gewährleistung eines hohen Sicherheitsniveaus in Kritischen Infrastrukturen hängt maßgeblich von der Vertrauenswürdigkeit eingesetzter Systeme, Komponenten und Dienstleistungen ab. Auch wenn gesetzliche IT-Sicherheitsanforderungen primär an Betreiber adressiert sind, ergeben sich daraus in der Praxis substanzielle Anforderungen für Hersteller und Dienstleister entlang der Lieferkette.

Als praxisnaher Leitfaden hat sich insbesondere das BDEW-Whitepaper „Anforderungen an sichere Steuerungs- und Telekommunikationssysteme“ (BDEW, 2024) etabliert. Es richtet sich ausdrücklich nicht nur an KRITIS-Betreiber, sondern auch an Hersteller und Dienstleister, die in sicherheitsrelevante Prozesse eingebunden sind. Das Whitepaper bietet konkrete Empfehlungen zur Ausgestaltung der Zusammenarbeit, zur Klärung von Rollen und Verantwortlichkeiten, zu vertraglichen Regelungen und zur standardisierten Bereitstellung sicherheitsrelevanter Informationen. Es enthält zudem Checklisten und Referenzmaßnahmen für ISMS-Prozesse, Systemhärtung, Patch-Management und den Austausch von Schwachstelleninformationen. Damit ist es eine wichtige Orientierungshilfe für die Umsetzung von Sicherheitsanforderungen nach dem „Stand der Technik“.

Pflichten für Hersteller: Zulassung und Zertifizierung im Fokus

Eine unmittelbare gesetzliche Pflicht zur Umsetzung technischer Sicherheitsmaßnahmen besteht für Hersteller und Dienstleister nur in bestimmten Konstellationen:

§ 9b BSIG fordert für sogenannte kritische Komponenten eine Zulassung durch das BSI. Voraussetzung hierfür ist die Abgabe einer Garantieerklärung durch den Hersteller, in der die Vertrauenswürdigkeit des Produkts bestätigt wird. Der Betreiber darf solche Komponenten nur dann einsetzen, wenn eine gültige Zulassung vorliegt. Die Pflicht zur Anzeige des Einsatzes und zur Berücksichtigung im Rahmen der Nachweisführung obliegt dabei dem Betreiber.

Auch im Messstellenbetrieb bestehen direkte gesetzliche Anforderungen für Hersteller. § 24 MsbG bestimmt, dass Smart Meter Gateways nur dann eingesetzt werden dürfen, wenn sie vom BSI zertifiziert wurden. Die Zertifizierung erfolgt auf Grundlage der Technischen Richtlinie TR-03109 sowie eines Schutzprofils nach den Common Criteria (CC) (BSI-CC-PP-0073) (BSI-1, 2019). Damit ist für diese Herstellergruppe ein strukturiertes Sicherheitsnachweissystem etabliert, das umfangreiche Prüfungen technischer, kryptografischer und organisatorischer Aspekte umfasst.

In den meisten Fällen ergeben sich die Anforderungen an Hersteller und Dienstleister jedoch mittelbar aus den Nachweispflichten der Betreiber. § 8a BSIG verpflichtet KRITIS-Betreiber zum Nachweis der Umsetzung angemessener technischer und organisatorischer Vorkehrungen zur IT-Sicherheit. In diesem Zusammenhang müssen Betreiber gegenüber dem BSI darlegen, dass alle eingesetzten Systeme, Komponenten und Dienstleistungen dem „Stand der Technik“ entsprechen. Diese Nachweispflicht führt dazu, dass Hersteller und Dienstleister zunehmend zur Bereitstellung von sicherheitsrelevanten Nachweisen, technischen Dokumentationen, Patch-Konzepten, Auditberichten oder Konformitätserklärungen verpflichtet werden, auch ohne ausdrückliche gesetzliche Regelung.

Die Einhaltung des „Stands der Technik“ orientiert sich an verschiedenen normativen Vorgaben. Dazu zählen beispielsweise Technische Richtlinien des BSI wie TR-02102 (kryptografische Verfahren) (BSI-2, 2025), TR-03109 (Smart-Meter-Infrastrukturen) (BSI-1, 2024) und TR-03116 (sichere Netzkommunikation) (BSI, 2018), internationale Normen wie ISO/IEC 27001 (ISMS) (BSI-2, 2019), ISO/IEC 27034 (sichere Softwareentwicklung) (BSI, 2021) und ISO/IEC 15408 (Common Criteria) (BSI-1, 2022) sowie Branchenspezifische Standards wie European Telecommunication Standards Institute (ETSI) EN 303 645 (IoT-Sicherheit) (ETSI, 2020).

Auch das allgemeine Produktsicherheitsrecht spielt eine zunehmende Rolle. Gemäß § 3 Abs. 1 Produktsicherheitsgesetz (ProdSG) dürfen Produkte nur in den Verkehr gebracht werden, wenn sie bei bestimmungsgemäßer Verwendung die Sicherheit und Gesundheit von Personen nicht gefährden. Diese Verpflichtung schließt heute auch die IT-Sicherheit ein. Ergänzend fordert die RED-Richtlinie (Radio Equipment Directive) (2014/53/EU) für bestimmte Funkanlagen, dass sie personenbezogene Daten schützen, Netzintegrität sicherstellen und über eine sichere Update-Funktion verfügen müssen. Die Verordnung (2022/30/EU) konkretisiert diese Anforderungen weiter.

Zukünftig wird auch europäische Regulierung die Anforderungen an Nachweise in der Lieferkette verschärfen. Die NIS2-Richtlinie verpflichtet erstmals auch IT-Dienstleister mit kritischen Aufgaben, etwa Hosting oder Softwarewartung, zur Einführung eines ISMS, zur Meldung von Sicherheitsvorfällen und zur Einhaltung aufsichtsrechtlicher Vorgaben. Der geplante CRA sieht zudem verpflichtende Sicherheitszertifizierungen für ausgewählte IT-Produkte vor, insbesondere für softwarebasierte Steuerungen und Netzwerkkomponenten. Eine aktuelle Übersicht über die daraus resultierenden Anforderungen sowie ihre Zuordnung zu bestehenden Normen bietet das Mapping-Dokument der European Union Agency for Cybersecurity (ENISA) zum CRA (ENISA, 2024).

2.4 Von der Verpflichtung zum Zertifikat

Die regulatorischen Anforderungen und relevanten Sicherheitsstandards wurden in Kapitel 2.1 und 2.2 bereits systematisch erläutert. Für den nachfolgenden Überblick über den Zertifizierungsprozess werden die wesentlichen Schnittstellen zu § 11 EnWG und § 8a BSIG nochmals fokussiert dargestellt.

2.4.1 Zertifizierungsprozesse nach § 11 EnWG

Die Verpflichtung zur Einführung eines ISMS ergibt sich im Energiewirtschaftsgesetz in zwei Ausprägungen:

- § 11 Abs. 1a EnWG richtet sich an Betreiber von Energieversorgungsnetzen, zum Beispiel Strom- und Gasnetzbetreiber mit Lizenz gemäß § 3 EnWG.

- § 11 Abs. 1b EnWG betrifft Betreiber von Energieanlagen, sofern diese als systemrelevant für die Versorgungssicherheit eingestuft werden, etwa Kraftwerke, Speicher oder zentrale Erzeugungseinheiten.

Beide Gruppen sind gesetzlich verpflichtet, „angemessene technische Vorkehrungen und sonstige Maßnahmen“ zum Schutz vor IT-basierten Bedrohungen zu treffen. Die konkrete Ausgestaltung dieser Anforderungen erfolgt über IT-Sicherheitskataloge, die von der BNetzA im Einvernehmen mit dem BSI veröffentlicht werden. Zur operativen Umsetzung des Zertifizierungsverfahrens hat die BNetzA ergänzend ein Konformitätsbewertungsprogramm (KBP) entwickelt. Es basiert auf der internationalen Norm ISO/IEC 17021 und enthält Vorgaben zur Auditpraxis, zur Qualifikation der Auditierer und zur Organisation von Zertifizierungsstellen.

Die Deutsche Akkreditierungsstelle (DAkkS) ist für die praktische Umsetzung des KBP verantwortlich. Sie überprüft im Rahmen der Akkreditierung regelmäßig, ob die Zertifizierungsstellen die im KBP festgelegten Anforderungen einhalten. Nur solche Stellen, die sowohl ISO/IEC-17021-konform arbeiten als auch die sektorenspezifischen Vorgaben der BNetzA erfüllen, dürfen entsprechende ISMS-Zertifizierungen nach IT-Sicherheitskatalog durchführen. In der Praxis beauftragt der Betreiber eine solche akkreditierte Zertifizierungsstelle, die ein Auditteam zusammenstellt. Dieses prüft die Erfüllung der Anforderungen aus dem jeweils einschlägigen IT-Sicherheitskatalog sowie der Norm ISO/IEC 27001, bei Energieanlagen ergänzt um die branchenspezifische Norm ISO/IEC 27019. Die Auditierung umfasst sowohl eine Dokumentenprüfung als auch eine Vor-Ort-Begutachtung.

Ein zentrales Merkmal des Verfahrens ist die Anwesenheit einer Fachexpertin bzw. eines Fachexperten im Auditteam. Diese Fachperson unterstützt das Audit bei der Beurteilung des ISMS-Scopes und der Risikoeinschätzung, insbesondere bei der Erst- und Rezertifizierung sowie bei Überwachungsaudits. Die Fachexpertinnen und -experten müssen über eine technische oder naturwissenschaftliche Qualifikation auf dem Niveau 6 des Deutschen Qualifikationsrahmens (DQR), mindestens drei Jahre einschlägige Berufserfahrung im Energiesektor sowie tiefgehende Kenntnisse der jeweiligen Anlagen- oder Netztechnologien verfügen. Unter bestimmten Bedingungen, etwa nach dokumentierter mehrfacher Begleitung durch eine Fachperson, kann ihre Anwesenheit in späteren Audits entfallen. Auditierer, die selbst alle Anforderungen erfüllen, können den Status „Fachexpertin“ bzw. „Fachexperte“ direkt erlangen.

Alle eingesetzten Auditierer müssen zudem eine von der BNetzA anerkannte Vollschulung mit abschließender Prüfung absolvieren. Diese Schulung dauert mindestens fünf Tage und umfasst unter anderem (i) rechtliche Rahmenbedingungen im Energiesektor, (ii) technische Grundlagen des Netz- und Anlagenbetriebs sowie (iii) Schwerpunkte zu ISMS-Strukturen gemäß IT-Sicherheitskatalog. Für Auditierer im Anlagenbereich ist zusätzlich eine zweitägige Aufbauschulung mit Spezialisierung auf Energieanlagentechnologien erforderlich. Eine regelmäßige Fortbildung im Dreijahresrhythmus (mindestens zehn Zeitstunden) stellt die kontinuierliche Qualifikation sicher.

Im Verlauf des Audits identifizieren die Auditierer etwaige Nichtkonformitäten, die in zwei Kategorien unterteilt werden:

- Abweichungen (Major Non-Conformities) bezeichnen schwerwiegende Mängel, etwa das Fehlen vorgeschriebener Maßnahmen oder systemische Schwächen, die die Wirksamkeit des ISMS gefährden.
- Nebenabweichungen (Minor Non-Conformities) beziehen sich auf kleinere Unvollständigkeiten oder formale Mängel, die keinen unmittelbaren Einfluss auf das Gesamtsystem haben, aber dennoch behoben werden müssen.

Nach Abschluss der Prüfung erstellt die Zertifizierungsstelle einen Auditbericht und entscheidet über die Erteilung des Zertifikats. Dieses dient als formalisierter Nachweis gegenüber der BNetzA. Liegen Abweichungen vor, ist eine Zertifizierung in der Regel erst nach ihrer Korrektur möglich; Nebenabweichungen können innerhalb definierter Fristen (z. B. im ersten Überwachungsaudit) nachdokumentiert werden.

Zusätzlich besteht eine Meldepflicht der Zertifizierungsstelle gegenüber der BNetzA: Jeweils zum 30. Juni und 31. Dezember eines Jahres muss eine aktualisierte Liste aller zertifizierten Unternehmen elektronisch übermittelt werden, selbst wenn sich keine Änderungen ergeben haben. Die Liste muss einem festgelegten Tabellenformat entsprechen, unter anderem mit Angaben zu Marktstammdaten, Zertifikatsnummer und Ablaufdatum. Auch ausgesetzte oder widerrufene Zertifikate sind gesondert auszuweisen.

Der vollständige Ablauf, von der Regelfestlegung über die Qualifikation von Auditierern bis zur Nachweisführung, ist in Abbildung 1 schematisch dargestellt. Die Grafik veranschaulicht die institutionellen Rollen sowie die Prozesslogik im Zertifizierungssystem gemäß § 11 EnWG.

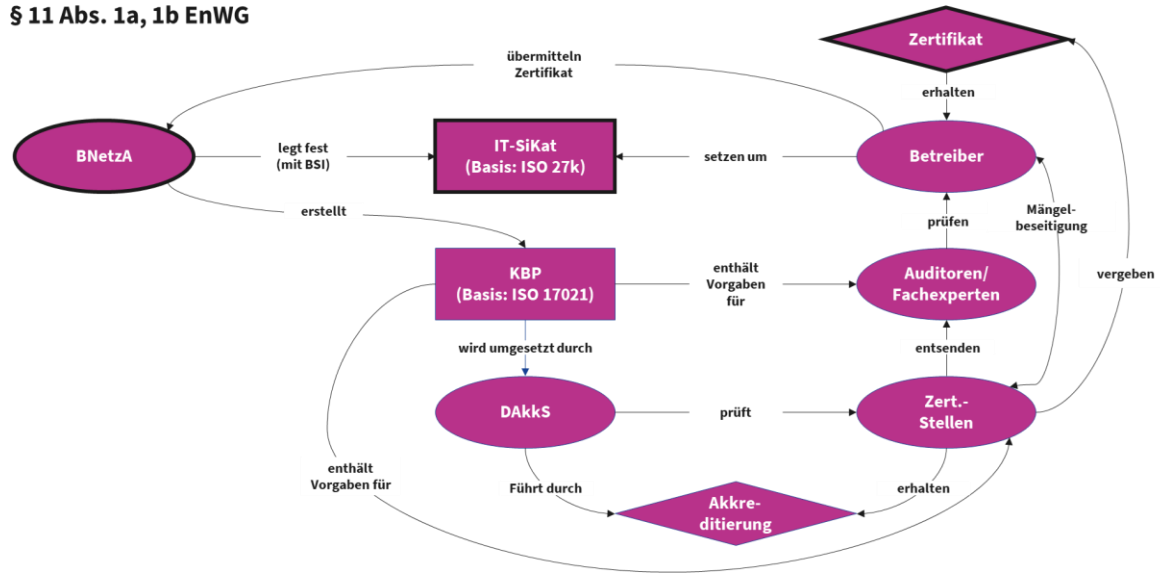

Abbildung 1: Zertifizierungsprozess nach § 11 Abs. 1a und 1b EnWG (eigene Darstellung auf Grundlage der Struktur der BNetzA)

2.4.2 Nachweisverfahren nach § 8a BSIG

Das Nachweisverfahren nach § 8a BSIG (Bundesrepublik Deutschland, 2023) richtet sich an Betreiber Kritischer Infrastrukturen, die verpflichtet sind, angemessene organisatorische und technische Maßnahmen zur Absicherung ihrer IT-Systeme umzusetzen. Ziel ist der Schutz vor Störungen, die erhebliche Auswirkungen auf die Versorgungssicherheit oder die öffentliche Sicherheit haben können. Das Verfahren gilt für Betreiber Kritischer Infrastrukturen gemäß BSI-KritisV (vgl. Kapitel 2.1).

Betreiber müssen dem BSI alle zwei Jahre einen Nachweis über die Umsetzung solcher Schutzmaßnahmen vorlegen. Dieser Nachweis wird durch eine vom BSI anerkannte Prüfstelle erstellt, die eine erfolgreiche Beteiligung am GAiN Verfahren (Grundsätzliche Anforderungen im Nachweisverfahren) sowie einschlägige Prüfkompetenz und Branchenerfahrung nachweisen muss (BSI-1, 2025).

Die Prüfung erfolgt auf Basis eines standardisierten Prüfrahmens, der auf die Erstellung strukturierter Nachweisdokumente (PE-Dokumente) ausgerichtet ist. Abweichungen werden im Rahmen der Prüfung als

wesentliche oder geringfügige Mängel dokumentiert. Anders als bei klassischen Auditprozessen ist im BSIG-Verfahren eine vollständige, nachvollziehbare Begründung aller Bewertungen durch die Prüfstelle erforderlich. Dies gilt insbesondere für die fachliche Begründung der Angemessenheit der Maßnahmen (PE.A), in der die Prüferinnen und Prüfer argumentativ darlegen, warum Maßnahmen im jeweiligen betrieblichen Kontext als angemessen gelten.

Trotz fehlender Zertifizierungs- oder Schulungspflicht erfolgt die Qualitätssicherung über die individuelle Anerkennung im GAiN-System. Die Anerkennung durch das BSI ist an personen- und organisationsbezogene Nachweise gebunden: Dazu zählen dokumentierte Prüferfahrungen, fundierte Kenntnisse relevanter Sicherheitsstandards (z. B. ISO/IEC 27001, BSI-Grundschutz) sowie eine belastbare Branchenerfahrung. Eine sicherheitsrechtliche Überprüfung nach dem Sicherheitsüberprüfungsgesetz (SÜG) ist nicht vorgeschrieben. Die Vertrauenswürdigkeit der Prüferinnen und Prüfer wird vielmehr über Berufspraxis, Referenzen und die regelmäßige Überprüfung durch das BSI abgesichert. Die Einreichung des Nachweises erfolgt elektronisch an das BSI. Dort wird geprüft, ob die Nachweisdokumente inhaltlich vollständig und fachlich nachvollziehbar sind. Das BSI kann Rückfragen stellen, Nachbesserungen einfordern oder die Nachweise zurückweisen. Eine formale Zertifikatserteilung ist nicht vorgesehen, die behördliche Anerkennung erfolgt durch implizite Akzeptanz des Nachweises.

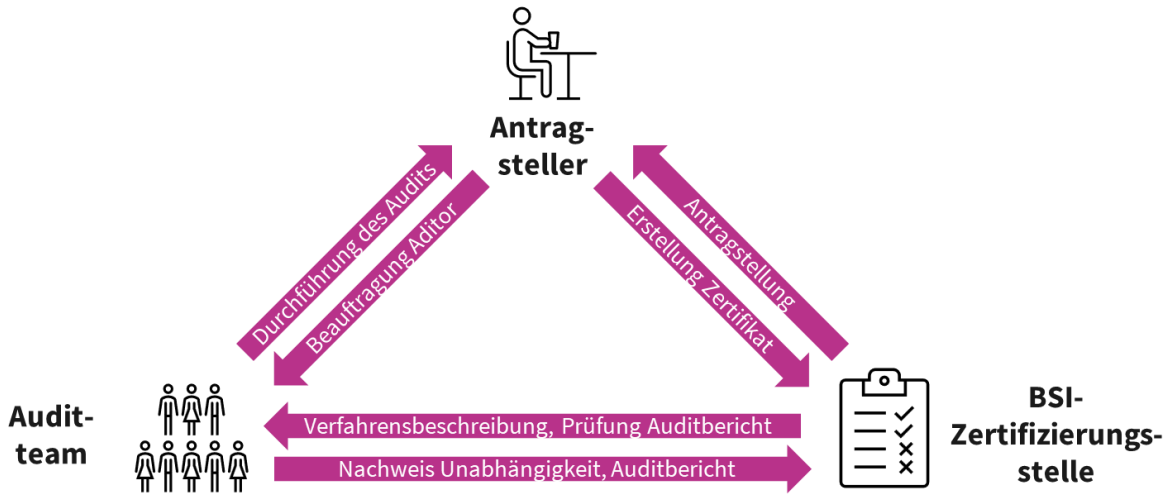

Abbildung 2: ISO-27001-Zertifizierungsverfahren auf Basis des BSI-IT-Grundschutzes (BSI-2, 2019)

Bereits bestehende ISMS können in das Nachweisverfahren eingebunden werden, sofern ihre dokumentierte Umsetzung zur Zielerreichung gemäß § 8a BSIG beiträgt. Dies ist insbesondere bei ISO/IEC-27001-Zertifizierungen, Audits im Trusted Information Security Assessment Exchange (TISAX) oder Systemen nach dem BSI-Grundschutz-Kompendium möglich. Entscheidend ist jedoch nicht die Zertifizierung an sich, sondern die inhaltliche Nachvollziehbarkeit und die Integration in die strukturierte Nachweisdokumentation.

Hinweis zur Abgrenzung: BSI-Grundschutz-Zertifizierung

Neben dem gesetzlich vorgeschriebenen Nachweisverfahren nach § 8a BSIG existiert beim BSI ein eigenständiges, freiwilliges **Zertifizierungsverfahren auf Basis des IT-Grundschutz-Kompendiums** (BSI, 2023). Es richtet sich an alle Organisationen, unabhängig von der KRITIS-Einstufung, und dient der strukturierten Prüfung eines ISMS. Der Antrag erfolgt direkt beim BSI und die Prüfung durch ein Auditteam, die Zertifikatserteilung wiederum durch das BSI selbst (vgl. Abbildung 2).

Dieses Verfahren ist **nicht identisch** mit dem Nachweisverfahren nach § 8a BSIG, kann aber als **Prüfbasis** herangezogen werden, sofern es nachvollziehbar in die Nachweisdokumentation (PE-Dokumente) eingebunden wird.

2.4.3 BSI-Zertifizierungen nach Technischen Richtlinien

Neben dem Nachweisverfahren nach § 8a BSIG und der freiwilligen IT-Grundschutz-Zertifizierung bietet das BSI eine Reihe von Zertifizierungsverfahren auf Basis Technischer Richtlinien (TR) an. Sie richten sich nicht ausschließlich an Betreiberorganisationen, sondern an Hersteller und Anbieter sicherheitskritischer IT-Produkte, Komponenten und Dienstleistungen. Im Gegensatz zu den zuvor beschriebenen Verfahren steht bei den TR-basierten Zertifizierungen nicht das Managementsystem im Mittelpunkt, sondern die Konformität eines Produkts oder Prozesses mit spezifischen technischen Anforderungen. Die Zertifizierungsverfahren orientieren sich dabei an einem festen Verfahrensablauf, der in der Verfahrensbeschreibung VB-Produkte.PD (BSI-2, 2024) geregelt ist: (i) Antragstellung beim BSI, (ii) Auswahl einer anerkannten Prüfstelle durch den Antragsteller, (iii) Durchführung der Konformitätsprüfung gemäß TR durch die Prüfstelle, (iv) Erstellung eines Prüfberichts und (v) Bewertung und Entscheidung über die Zertifikatserteilung durch die BSI-Zertifizierungsstelle.

Die Technischen Richtlinien definieren jeweils einen klar umrissenen Prüfgegenstand sowie die anzuwendenden Testmethoden und Bewertungskriterien. Beispiele sind die TR-03109 (intelligente Messsysteme) (BSI-1, 2024), TR-03122 (Biometrie) (BSI-2, 2022), TR-03130 (eID-Server) (BSI-1, 2020) oder TR-03124 (eID-Client) (BSI-2, 2020). Die Prüfungen betreffen Software- oder Hardwarekomponenten und umfassen funktionale Sicherheitsanforderungen, kryptografische Mechanismen und Interoperabilität.

Zur Durchführung der Prüfungen werden vom BSI produktspezifisch anerkannte Prüfinstanzen benannt. Eine Akkreditierung durch die DAkkS ist hierfür nicht zwingend erforderlich. Stattdessen erfolgt die Anerkennung über eine individuelle Bewertung der Prüfstelle durch das BSI, bezogen auf (i) fachliche Eignung im jeweiligen Technologiefeld, (ii) Kenntnis und Anwendungssicherheit in Bezug auf die jeweilige TR, (iii) Nachweis einschlägiger Prüferfahrungen und (iv) Vertrautheit mit den Prüfmethoden.

Für bestimmte Verfahren, etwa die Zertifizierung von Smart Meter Gateways gemäß TR-03109, verlangt das BSI zusätzlich den Einsatz eigens anerkannter TR-Auditierer, die durch das BSI geprüft wurden und den Abgleich mit der Norm ISO/IEC 27001 im Zusammenspiel mit der TR vornehmen können. Eine DAkkS-Akkreditierung der Zertifizierungsstellen ist zwar zulässig, wird aber vom BSI nicht zwingend vorgeschrieben und ersetzt nicht die inhaltliche Anerkennung des Prüfpersonals durch die Fachabteilungen des BSI.

Die Qualitätssicherung innerhalb dieser Verfahren erfolgt nicht über ein zentrales Konformitätsbewertungsprogramm wie bei der BNetzA, sondern durch (i) formalisierte TR-Prüfkataloge, (ii) definierte Prüfberichtformate sowie (iii) die abschließende Prüfung und Entscheidung durch die BSI-Zertifizierungsstelle.

Die ausgestellten Zertifikate sind öffentlich abrufbar und kennzeichnen Produkte oder Komponenten, die spezifische Anforderungen der jeweiligen Technischen Richtlinie erfüllen. Je nach Anwendungsbereich dienen sie als Voraussetzung für den Marktzugang und regulatorische Freigaben oder als Bestandteil von Gesamtarchitekturen in sicherheitskritischen Infrastrukturen.

Für Energieversorgungsunternehmen ergibt sich eine Verpflichtung zur Einhaltung TR-bezogener Anforderungen insbesondere dann, wenn sie Komponenten einsetzen, deren Einsatz regulatorisch an eine BSI-Zertifizierung gebunden ist, etwa bei intelligenten Messsystemen gemäß TR-03109, bei sicherheitsrelevanten Kommunikationsmodulen oder bei eID-Anwendungen in der Marktkommunikation. Die Unternehmen selbst fungieren dabei nicht als Zertifizierungsadressaten, sondern müssen nachgelagert sicherstellen, dass sie ausschließlich zertifizierte Produkte einsetzen, sofern dies gesetzlich (z. B. im Messstellenbetriebsgesetz) oder durch Festlegungen der BNetzA vorgeschrieben ist.

Die TR-Zertifizierungen betreffen somit primär Hersteller, entfalten aber über nutzungsbezogene Vorgaben auch eine mittelbare Bindungswirkung für Energieversorgungsunternehmen, insbesondere im Fall gesetzlich geregelter Systemlandschaften wie dem Smart Meter Rollout. Damit bilden die TR-basierten Zertifizierungen eine ergänzende Regulierungsebene, die auf technische Komponenten zielt, aber im Zusammenspiel mit EnWG- und BSIG-Verfahren das Gesamtsystem absicherungsrelevant prägt. Diese Zertifizierungsverfahren ergänzen damit die managementsystemorientierten Nachweis- und Auditverfahren um eine technikzentrierte Bewertungsebene, in der das BSI regulatorische, prüfende und zertifizierende Funktionen in einem Gesamtprozess bündelt.

2.4.4 Gegenüberstellung der Verfahren

Die in den Kapiteln 2.4.1 bis 2.4.3 beschriebenen Verfahren zur IT-sicherheitsbezogenen Nachweisführung und Zertifizierung unterscheiden sich in ihrer Zielsetzung, methodischen Umsetzung und institutionellen Verankerung erheblich. Während sie alle zur Absicherung kritischer digitaler Systeme beitragen, folgen sie unterschiedlichen Governance-Logiken, Prüfansätzen und Regulierungswegen. Die in Tabelle 3 dargestellte strukturierte Gegenüberstellung verdeutlicht Gemeinsamkeiten, Unterschiede und mögliche Reibungsflächen.

Das EnWG-Verfahren zielt auf eine formale Zertifizierung des ISMS und wird durch ein akkreditiertes, international anschlussfähiges Auditmodell getragen. Es ist hoch strukturiert, basiert auf einem öffentlich dokumentierten KBP und wird durch die BNetzA als Aufsichtsbehörde überwacht.

	EnWG-Zertifizierung (§ 11 EnWG, BNetzA)	Nachweisverfahren (§ 8a BSIG, BSI)	TR-Zertifizierung (Technische Richtlinien, BSI)
Rechtsgrundlage	§ 11 Abs. 1a und 1b EnWG	§ 8a BSIG	IT-Sicherheitsgesetz i. V. m. TR
Adressaten	Netz- und Anlagenbetreiber	KRITIS-Betreiber	Hersteller von IT-Produkten und -Komponenten
Zielrichtung	ISMS-Zertifizierung auf Basis IT-Sicherheitskatalog	Nachweis angemessener Sicherheitsmaßnahmen	Konformitätsnachweis zu technischen Sicherheitsanforderungen
Prüforganisation	DAkkS-akkreditierte Zertifizierungsstelle und KBP der BNetzA	Prüferinnen und Prüfer mit GAiN-Anerkennung	Anerkannte Prüfinstanzen (produktspezifisch)
Aufsicht / Koordination	BNetzA	BSI	BSI

	EnWG-Zertifizierung (§ 11 EnWG, BNetzA)	Nachweisverfahren (§ 8a BSIG, BSI)	TR-Zertifizierung (Technische Richtlinien, BSI)
Formaler Nachweis	Zertifikat nach ISO/IEC 27001 und IT-Sicherheits-katalog	PE-Dokumente, keine Zertifizierung	BSI-Zertifikat (TR-spezifisch)
Zertifizierungsziel	Unternehmens-ISMS	Umsetzung sicherheitsrelevanter Maßnahmen	Produktsicherheit, Interopera-bilität
Standardbezug	ISO/IEC 27001 und 27019	Optional: ISO/IEC 27001 oder Grundschutz	TR-Anforderungen, ggf. ISO/IEC 27001 ergänzend
Prüferqualifikation	ISO/IEC 17021, KBP-Schu-lung, DAkkS-Auditteam	GAiN-Anerkennung, Nach-weise über Erfahrung	TR-Fachexpertise, projektspezi-fische Anerkennung durch das BSI
Externe Aufsicht / Akkreditierung	Ja (DAkkS)	Nein	Teilweise, bei Bedarf

Tabelle 3: Strukturelle Merkmale und Unterschiede zentraler Auditverfahren im KRITIS- und Energiekontext

Das Verfahren nach § 8a BSIG dagegen ist inhaltlich offener gestaltet. Es stützt sich auf einen individuellen, risikobasierten Nachweisansatz mit prüferischer Begründungstiefe, verzichtet aber auf Zertifikate oder formale ISO-Audits. Die Qualitätssicherung erfolgt durch das BSI selbst im Rahmen der GAiN-Struktur und durch die inhaltliche Prüfung der PE-Dokumente.

Die TR-basierten Verfahren des BSI konzentrieren sich hingegen auf konkrete technische Produkte oder Komponenten. Die Prüfmethodik ist stark spezifikationsgeleitet, das Prüfpersonal wird durch das BSI pro Programmbereich zugelassen. Eine zentrale Akkreditierung entfällt. Zertifikate werden durch das BSI oder benannte Stellen auf Basis formalisierter Prüfberichte ausgestellt.

Für Energieversorgungsunternehmen entsteht dadurch ein komplexes Nebeneinander von Anforderungen: Während ISMS-Zertifizierungen nach § 11 EnWG verpflichtend sind und gegebenenfalls mit einem freiwilligen Grundschutz-Zertifikat ergänzt werden, müssen bestimmte Produkte, etwa Smart Meter Gateways, zusätzlich TR-zertifiziert sein. Betreiber, die zugleich KRITIS-relevant sind, unterliegen dem Nachweisregime nach § 8a BSIG. Das führt zu parallelen Prüfzyklen, uneinheitlichen Bewertungsmaßstäben und voneinander abweichenden Nachweisdokumenten. Insbesondere in der operativen Umsetzung treten damit medien- und prozessbruchhafte Strukturen zutage: Die Erfüllung gleichartiger Anforderungen (z. B. zur Risikoanalyse, zum Patch-Management oder zur Angriffserkennung) muss mehrfach, aber in unterschiedlicher Form nachgewiesen werden. Eine systematische Verzahnung der Prüf- und Anerkennungsverfahren besteht bislang nicht.

2.5 Harmonisierungspotenziale bestehender Zertifizierungen

Angesichts der unterschiedlichen regulatorischen Verfahren zur IT-Sicherheitszertifizierung in Deutschland stellt sich die Frage, in welchen Bereichen sich Synergien erschließen lassen, um Doppelarbeit zu vermeiden und Ressourcen effizienter einzusetzen. Harmonisierung bedeutet in diesem Kontext nicht die Vereinheitlichung aller Verfahren, sondern die gezielte Identifikation von Schnittmengen, die wechselseitige Anerkennung funktional äquivalenter Nachweise und die strukturelle Abstimmung von Prüfprozessen.

2.5.1 Strukturprobleme und Praxisbedarfe in bestehenden Zertifizierungsverfahren

Trotz inhaltlicher Überschneidungen zwischen verschiedenen IT-Sicherheitsanforderungen erleben Unternehmen die gegenwärtige Nachweis- und Zertifizierungslandschaft als fragmentiert, teilweise widersprüchlich und ineffizient. Die Herausforderungen reichen dabei von unklaren Zuständigkeiten über uneinheitliche Prüfanforderungen bis hin zu auditbedingten Redundanzen. Die folgenden Praxisbedarfe und Reibungspunkte wurden im Rahmen eines Workshops der Branchenplattform Cybersicherheit identifiziert und verdichtet. Im Folgenden werden sie systematisch dargestellt.

Unterschiedliche Zielrichtungen und Nachweislogiken: Die untersuchten Verfahren – EnWG-Zertifizierung, Nachweis nach § 8a BSIG und TR-Zertifizierungen – verfolgen unterschiedliche Absichten: formalisierte Zertifikate, risikobasierte PE-Bewertungen und komponentenbezogene Konformitätsnachweise. Diese divergierenden Prüfziele führen zu Inkompatibilitäten bei Auditaufbau, Nachweisstruktur und Prüferwartung.

Unklare Rollenzuweisung zwischen Behörden und Verfahren: In der Praxis besteht vielfach Unsicherheit darüber, welche Anforderungen durch BNetzA, BSI oder Zertifizierungsstellen jeweils gesetzt und bewertet werden. Der Prüfprozess ist nicht kohärent orchestriert. Besonders bei Organisationen, die mehreren Regimen unterliegen (z. B. Netzbetrieb plus KRITIS-Rolle plus Produktverantwortung), führt dies zu Abgrenzungsproblemen und Doppelverantwortlichkeiten.

Unvereinbare Anforderungen an Prüfpersonen: Während ISO/IEC 17021 und KBP eine standardisierte Auditorenqualifikation verlangen, genügt im Kontext von § 8a BSIG die individuelle GAiN-Anerkennung durch das BSI. TR-Zertifizierungen wiederum setzen auf produktspezifische Expertise ohne formales Akkreditierungssystem. Diese Unterschiede erschweren kombinierte Audits und lassen Zweifel an der Vergleichbarkeit der Ergebnisse entstehen.

Unnötige Mehrfachprüfung gleichartiger Kontrollen: Kontrollen wie Risikomanagement, Zugriffssteuerung oder Backup-Strategien müssen in unterschiedlichen Formaten dokumentiert werden: als Auditbericht, PE.A-Begründung oder TR-Prüfbericht. Da Format, Detailtiefe und Bewertungsmaßstab variieren, kommt es zu doppelter Arbeit, sowohl bei der Prüfung als auch bei der Vorbereitung.

Fehlende Scoping-Klarheit und zu hoher Dokumentationsaufwand: Unternehmen berichten von hohem Aufwand für Auditvorbereitungen und Nachweiserstellung. Oft fehlt eine eindeutige Abgrenzung:

Es stellt sich die Frage, welche Rollen und Geltungsbereiche betroffen sind, etwa bei der Unterscheidung zwischen Gateway Administrator (GWA) und CLS-Management (Controllable Local System) im Smart-Metering-Kontext. Obwohl beide über das Smart Meter Gateway interagieren, gelten unterschiedliche Zuständigkeiten und Prüfkriterien.

- Was ist prüfrelevant, was nur begleitend?
- Wie lange gelten dokumentierte Nachweise? Welche Formate sind erforderlich?

Mangel an OT-bezogener Auditierungskompetenz: Mehrere Praxisakteure berichteten, dass in Audits nach § 11 EnWG sowie nach § 8a BSIG häufig eine unzureichende Berücksichtigung von OT-spezifischen Anforderungen festzustellen sei. Obwohl viele sicherheitskritische Systeme, etwa in der Energieinfrastruktur, auf industriellen Steuerungstechnologien basieren, erfolgt die Bewertung oft primär aus IT-Perspektive. Insbesondere der praktische Umgang mit Netzleittechnik oder Fernwirktechnik wird nach Einschätzung der Beteiligten nicht adäquat abgebildet.

Während im EnWG-Verfahren zumindest über das Konformitätsbewertungsprogramm gewisse Qualifikationsvorgaben für Auditierer bestehen, fehlen solche Anforderungen im Verfahren nach § 8a BSIG vollständig. Dort erfolgt die Prüferauswahl über individuelle GAiN-Anerkennungen, die keine Sektor- oder OT-spezifische Kompetenz voraussetzen. Im Unterschied dazu stellt das EnWG-Verfahren durch das KBP nicht nur sicher, dass qualifizierte Auditierer eingesetzt werden, sondern auch, dass die Bewertung anhand standardisierter Kriterien erfolgt. Durch klare Prüfentscheidungen (z. B. erfüllt / Abweichung) und strukturierte Anforderungslisten wird die Vergleichbarkeit und Nachvollziehbarkeit gestärkt, auch wenn Auditierer über unterschiedliche Erfahrungsgrade verfügen. Diese Systematik fehlt im Verfahren nach § 8a BSIG, das primär auf individuelle Einschätzungen der Prüferinnen und Prüfer und narrative Begründungen in PE-Dokumenten angewiesen ist.

Risikobasierte Prüfungen zwischen Flexibilität und Unsicherheit: Ein weiterer, häufig unterschätzter Reibungspunkt betrifft den risikobasierten Prüfansatz selbst. Obwohl er mehr Raum für kontextangepasste Lösungen bietet, sorgt er in der Praxis häufig für Unsicherheit, sowohl aufseiten der Betreiber als auch auf der der Prüferinnen und Prüfer. Ohne verbindliche Referenzmaßstäbe oder Entscheidungskategorien herrscht oftmals Unklarheit darüber, was als angemessene Maßnahme gilt. Aus Sorge vor Rechtsfolgen oder reputativen Risiken werden viele Risikobewertungen entweder gar nicht erst offen geteilt oder so defensiv formuliert, dass sie ihre eigentliche Wirkung verlieren. Ein möglicher Lösungsansatz liegt in einem hybriden Bewertungsmodell, das freie, textlich formulierte Begründungen risikobasierter Prüfungen mit nachvollziehbaren Bewertungskategorien (etwa aus dem KBP) verbindet und so sowohl die fachliche Tiefe als auch die Bewertungstransparenz sichert.

Unzureichende Verzahnung mit europäischem Regulierungsrahmen: Der zeitliche Verzug bei der Umsetzung harmonisierter europäischer Normen (z. B. RED, CRA, EUCC) erschwert Herstellern und Betreibern die Nachweisführung. Gleichzeitig bleibt offen, ob bestehende Zertifizierungen (z. B. ISO 27001, BSI-Grundschutz) im Kontext kommender Vorgaben weiterhin anerkannt werden oder überarbeitet werden müssen.

2.5.2 Verbesserungspotenziale und Handlungsansätze

Die Analyse der heutigen Zertifizierungslandschaft zeigt zahlreiche systemische Reibungspunkte und Ineffizienzen. Viele Betreiber sehen sich mit fragmentierten Anforderungen, mehrfachen Prüfzyklen und unklaren Bewertungskriterien konfrontiert. Daraus ergibt sich ein erheblicher administrativer Aufwand, nicht nur für Betreiber, sondern auch für Auditierer und Aufsichtsbehörden. Gleichzeitig liegen konkrete Ansatzpunkte für strukturelle und regulatorische Verbesserungen vor, die sich in sechs zentrale Handlungsfelder gliedern lassen.

1) Fragmentierung und Redundanz: Die Trennung zwischen verschiedenen Zertifizierungsregimen, etwa nach EnWG, § 8a BSIG oder Technischen Richtlinien, führt häufig zu Doppelprüfungen. Ein modular aufgebautes Zertifizierungssystem mit anschlussfähigen Grund- und Zusatzmodulen sowie die gegenseitige Anerkennung etablierter Standards wie ISO/IEC 27001 oder BSI-Grundschutz könnten hier substanzielle Entlastung schaffen. Auch die gezielte Wiederverwendung bereits geprüfter Prüfelemente würde den Aufwand reduzieren.

2) Uneinheitliche Bewertungsmaßstäbe: Risikobasierte Ansätze bieten zwar Flexibilität, führen in der Praxis jedoch oft zu Unsicherheiten bei der Prüfung und Nachweisführung. Die Einführung hybrider Prüfmodelle, zum Beispiel durch Mindestanforderungen zur Umsetzung sicherer Systeme,

SOLL/MUSS/WIRD-Kategorisierungen oder abgestimmten Kriterienkatalogen, und eine stärkere dialogische Rückkopplung mit Behörden können hier Abhilfe schaffen. Einheitliche Berichtsvorlagen und PE-Formate würden zusätzlich die Vergleichbarkeit verbessern.

3) Normenvielfalt und fehlende Mappings: Derzeit existieren kaum offizielle Mappings zwischen nationalen (§ 8a BSIG), internationalen (ISO/IEC) und europäischen (z. B. EUCS, EUCC, CRA) Standards. Diese Unverbundenheit erschwert nicht nur die Nachweispraxis, sondern auch die internationale Vergleichbarkeit. Klare Anrechnungstabellen und die verpflichtende Integration sektoraler Normen wie ISO/IEC 27019 würden die Praxisnähe und Kohärenz der Prüfungen erhöhen.

4) Inkompatible Produktzertifizierungen: Auch bei technischen Prüfungen von Komponenten und Systemen bestehen heute hohe Redundanzen, etwa zwischen BSI-TR, IEC 62443 und künftigen CRA-Vorgaben. Eine inhaltliche Harmonisierung der Prüfkataloge sowie die nationale Anerkennung gleichwertiger EU-Zertifikate würden den Aufwand für Hersteller reduzieren und die Sicherheitssystematik vereinheitlichen.

5) Fehlende Anerkennung kombinierter Nachweise: Viele Unternehmen lassen bereits mehrere Anforderungen in einem kombinierten Audit prüfen, zum Beispiel nach ISO 27001 und ISO 22301. Allerdings fehlt häufig die regulatorische Anerkennung solcher Kombi-Zertifikate. Eine formelle Zulassung dieser Bündelungen würde Synergien heben und Prüfzyklen reduzieren.

6) Transparenz und Qualifikation: Auch die Qualität und Sichtbarkeit von Zertifikaten kann verbessert werden. Einheitliche, verbindliche Qualifikationsstandards für Auditierer würden die Prüfqualität sichern. Der Aufbau europäischer Zertifikatsdatenbanken oder sicherer Austauschplattformen könnte zudem Redundanzen in der Nachweisführung verringern und die Vertrauensbasis stärken.

Insgesamt zeigen diese Handlungsfelder, dass die bestehenden Systeme nicht grundlegend ersetzt werden müssen, wohl aber stärker aufeinander abgestimmt, effizienter gestaltet und transparenter gemacht werden können. Eine gezielte Harmonisierung würde nicht nur den Prüfaufwand reduzieren, sondern auch die Resilienz und Kohärenz des Gesamtsystems stärken.

2.5.3 Regulatorischer Ausblick

Die Analyse der heutigen Zertifizierungslandschaft macht deutlich, dass bereits jetzt eine hohe Komplexität bei Prüf- und Nachweisverfahren besteht. Diese Landschaft wird sich in den kommenden Jahren nochmals dynamisch verändern: Mit der Umsetzung der NIS2-Richtlinie, des KRITIS-Dachgesetzes und des europäischen CRA stehen erhebliche Ausweitungen der Sicherheits- und Nachweispflichten bevor.

	Bisheriger Regulierungsstatus	Erweiterung durch NIS2 / KRITIS-DachG / CRA
KRITIS-Betreiber	ISMS-Pflicht, Prüfungen nach § 8a BSIG, Meldepflichten	Verbindliche Resilienzpläne, verschärfte Meldefristen (24h/72h), Lieferkettenverantwortung, Haftungsverschärfung
Nicht-KRITIS-Betreiber	ISMS nach „Stand der Technik“ (§ 11 EnWG), keine Zertifizierungspflicht	Pflicht zur ISMS-Zertifizierung (z. B. ISO 27001), neue Meldepflichten, Risikoanalyse für IT/OT
IT-Dienstleister mit Systemzugriff	Vertragsrechtlich gebunden über Betreiber	Direkte Regulierung (z. B. ISMS, Meldepflicht), behördliche Aufsicht durch das BSI

	Bisheriger Regulierungsstatus	Erweiterung durch NIS2 / KRITIS-DachG / CRA
Hersteller kritischer Produkte	Einzelregeln (z. B. SMGW, § 19 Abs. 1 MsbG)	Verpflichtende Produktzertifizierung, Patch-Pflicht, Schwachstellenmanagement nach CRA
Hersteller/Dienstleister ohne Systemzugriff	Bisher nicht reguliert, freiwillige Nachweise	Erwartung von Sicherheitsnachweisen (z. B. ISO 27001), Einbindung über Betreiberverant-wortung

Tabelle 4: Regulierungsdynamik entlang der energiewirtschaftlichen Wertschöpfungskette: erwartete Erweiterung von Pflichten und Nachweisanforderungen im Kontext von NIS2, KRITIS-Dachgesetz und Cyber Resilience Act

Besonders relevant ist dabei, dass sich die Pflichten systematisch auf Akteure unterhalb der bisherigen KRITIS-Schwelle sowie auf Hersteller und Dienstleister in der Lieferkette ausdehnen. Die bisherige Schwerpunktsetzung auf Betreiber Kritischer Infrastrukturen wird durch eine differenzierte, rollenbasierte Regulierung ergänzt, die auch indirekt involvierte Marktakteure einbezieht. Dazu zählen zum Beispiel IT-Dienstleister mit Zugang zu kritischen Systemen oder Anbieter von Standardsoftware, deren Produkte sicherheitsrelevante Funktionen erfüllen. Im Ergebnis führt dies zu einem regulatorischen Wandel, der eine konsequentere Integration der gesamten Lieferkette in das Cybersicherheits-Management erforderlich macht. Betreiber werden verstärkt dafür verantwortlich gemacht, die Sicherheit ihrer vorgelagerten Systeme und eingesetzten Komponenten nachzuweisen. Damit gewinnen auch Zertifizierungen jenseits des klassischen Kontexts von Betreibern erheblich an Bedeutung. Tabelle 4 zeigt, wie sich die Pflichten rollenabhängig verändern.

Zentrale Entwicklung

Die Grenze zwischen „direkt regulierten“ und „indirekt eingebundenen“ Akteuren verwischt. Künftig gilt für alle: Der „Stand der Technik“ in der Cybersicherheit wird zum nachweispflichtigen Mindeststandard, unabhängig von der eigenen Systemverantwortung.

2.6 Fazit und Handlungsperspektiven

Die Analyse zeigt, dass die aktuelle Zertifizierungslandschaft geprägt ist von hohen fachlichen Anforderungen, zugleich aber auch von struktureller Fragmentierung und begrenzter Anschlussfähigkeit zwischen einzelnen Verfahren. Die Vielzahl an Standards, Regimen und Zuständigkeiten führt zu Redundanzen, Unsicherheiten und vermeidbarem Aufwand, sowohl bei der Nachweisführung als auch in der Prüfungspraxis. Gleichzeitig lassen sich konkrete Ansatzpunkte identifizieren, an denen regulatorische, prozessuale oder strukturelle Verbesserungen ansetzen können (vgl. Tabelle 5).

Zentral erscheint dabei die Entwicklung eines kohärenten Prüfökosystems, das unterschiedliche Nachweis-formen nicht isoliert betrachtet, sondern strukturell aufeinander abstimmt. Die vorgestellten Handlungsfelder bieten hierfür konkrete Ansatzpunkte – von modularen Zertifizierungsarchitekturen über hybride Prüfmodelle mit regulatorischer Rückkopplung bis hin zur transparenten Wiederverwendung bestehender Nachweise. Ergänzend sind auch Maßnahmen wie die gegenseitige Anerkennung von ISMS-Zertifikaten (z. B. ISO/IEC 27001 und BSI-Grundschutz), die Einführung verbindlicher Qualifikationsstandards für Auditierer sowie der Aufbau europäischer Zertifikatsregister und Auditplattformen zur nachvollziehbaren Nachweisführung relevant.

	Empfohlene Maßnahme	Ziel/Nutzen
Fragmentierung und Redundanz in Nachweisen	Entwicklung modularer, anschlussfähiger Prüfverfahren; gegenseitige Anerkennung von ISMS-Zertifikaten (ISO/IEC 27001, BSI-Grundschutz); Referenzierung bestehender PE-Bausteine	Doppelprüfungen vermeiden, Effizienz steigern, Betreiber entlasten
Uneinheitliche Bewertungsmaßstäbe und Formate	Einführung hybrider Prüfmodelle (z. B. MUSS/SOLL/WIRD) mit dialogischer Aufsicht; Standardisierung von PE-Vorlagen und Auditberichten	Prüfbarkeit erhöhen, Vertrauen stärken, Klarheit schaffen
Unverbundene Normen und sektorale Anforderungen	Offizielle Mappings und Anrechnungstabellen zwischen Bausteinen nach § 8a, ISO-Normen, EUCC, CRA etc.; verbindliche Berücksichtigung sektoraler Normen (z. B. ISO/IEC 27019)	Internationale Vergleichbarkeit, realistische Abbildung von OT-Anforderungen
Zersplitterte Produktzertifizierungen	Harmonisierung technischer Prüfkataloge (z. B. BSI-TR, IEC 62443); Anerkennung EU-weiter Zertifikate bei gleichwertiger Schutzwirkung	Marktzugang vereinfachen, Prüfkosten senken, Qualität sichern
Uneinheitliche Auditorenstandards	Einführung verbindlicher Qualifikationsstandards (z. B. nach KBP-Vorbild mit Schulung und Referenzprüfung)	Vergleichbare Prüfqualität sicherstellen
Mangel an Sichtbarkeit und Nachvollziehbarkeit	Aufbau europäischer Zertifikatsdatenbanken; Auditplattformen für vertraulichen Austausch	Transparenz erhöhen, Nachweislast reduzieren

Tabelle 5: Kompaktdarstellung der identifizierten Harmonisierungspotenziale

Adressierte Akteure: Die in diesem Kapitel skizzierten Maßnahmen zur Harmonisierung von Prüfverfahren und Zertifizierungsregimen adressieren mehrere Verantwortungsebenen:

- Politik und Aufsichtsbehörden (z. B. BSI, BNetzA, BMWE) sind zuständig für die rechtliche Anerkennung paralleler Zertifizierungsschemata, die Einführung verbindlicher Qualifikationsstandards sowie den Aufbau übergreifender Prüfökosysteme.
- Branchenplattformen und -verbände sollten methodische Grundlagen, sektorübergreifende Mappings und PE-Bausteine entwickeln sowie die sektorinterne Rückkopplung organisieren.
- Auf europäischer Ebene ist insbesondere die ENISA gefordert, die Entwicklung und Etablierung technischer Rahmenwerke (EUCS, EUCC, CRA) sowie gemeinsamer Registerlösungen voranzutreiben.

Als Voraussetzung bleibt, dass die Harmonisierung nicht zur Absenkung von Schutzniveaus führen darf, sondern dort ansetzen muss, wo Prüfziele vergleichbar, Anforderungen deckungsgleich und Aufwände vermeidbar sind. Mit der ENISA steht bereits eine zentrale europäische Institution bereit, um die technischen, prozessualen und regulatorischen Grundlagen hierfür zu schaffen. Die Entwicklung und Etablierung EU-weiter Zertifizierungsschemata, wie EUCC, EUCS oder perspektivisch im Rahmen des CRA, sowie begleitender Registerplattformen für Nachweise und Auditergebnisse kann die bislang national fragmentierte Landschaft grundlegend strukturieren (ENISA, 2024; Europäische Union, 2024).

Kohärentes Prüfökosystem: Voraussetzung für Effizienz und Vertrauen

Ein kohärentes Prüfökosystem ist möglich, aber nur wenn nationale, sektorale und europäische Anforderungen strukturell aufeinander abgestimmt werden, ohne das Schutzniveau zu kompromittieren. Dazu braucht es modulare, anschlussfähige Prüfverfahren, verbindliche Auditorenstandards und transparente Registerlösungen.

Entscheidend wird sein, in welchem Maße es gelingt, nationale Anforderungen, sektorale Besonderheiten und europäische Harmonisierungsbestrebungen in ein konsistentes Gesamtsystem zu überführen. Wie sich die zuvor beschriebenen Fragmentierungen und Anforderungen im betrieblichen Alltag konkret auswirken und welche Herausforderungen sich beim Aufbau widerstandsfähiger Strukturen stellen, zeigt das folgende Kapitel anhand einer Fallstudie aus dem kommunalen Versorgungssektor. Es macht deutlich, wo bestehende Sicherheits-, Nachweis- und Resilienzstrukturen an Grenzen stoßen und welche systemischen wie operativen Konsequenzen daraus entstehen.

3 Fallstudie: Integriertes Stadtwerk mit Betrieb alter und neuer OT-Systeme

Ziel dieser Fallstudie ist es, ein fiktives integriertes Stadtwerk exemplarisch in jenem Spannungsfeld zwischen technischer Heterogenität, organisatorischer Verantwortung und wachsender regulatorischer Komplexität zu verorten, das für viele Versorgungsunternehmen in Deutschland zunehmend relevant wird. Durch die enge Verzahnung von Netzbetrieb, Energieerzeugung, Vertrieb und IT-/OT-Betrieb in einer gemeinsamen Organisationseinheit stellt das integrierte Stadtwerk eine besonders anschauliche Konstellation mit hoher Komplexität und vergleichsweise begrenzten Ressourcen dar.

Im Zentrum der Analyse stehen drei Leitfragen:

- Wie beeinflusst die technische Koexistenz alter OT-Systeme und moderner IT-Komponenten die Sicherheitsarchitektur und betriebliche Resilienz?
- Welche regulatorischen Anforderungen treffen ein Stadtwerk unterhalb der KRITIS-Schwelle?
- Wie kann ein integriertes Resilienzkonzept entwickelt werden, das über klassische ISMS-Ansätze hinausgeht und auch hybride Systemrisiken, organisatorische Abhängigkeiten und externe Lieferbeziehungen systematisch adressiert?

Dabei verfolgt die Studie keine vollständige Risikobewertung, sondern zielt auf eine strukturierte Identifikation zentraler Handlungsfelder und Gestaltungsoptionen ab. Die Fallstudie dient somit als praxisnaher Referenzrahmen, der auch übertragbar ist auf andere Organisationen mit vergleichbarer Systemlandschaft und Regulierungsbetroffenheit, insbesondere in der kommunalen Energieversorgung.

Unter einem integrierten Stadtwerk wird im Rahmen dieser Fallstudie eine Organisation verstanden, die zentrale Funktionen der kommunalen Energieversorgung, insbesondere Netzbetrieb, Energieerzeugung, Vertrieb, Messstellenbetrieb und den Betrieb von Steuerungs- und Kommunikationssystemen, in einer gemeinsamen Organisationseinheit bündelt. Anders als bei rechtlich entbündelten Strukturen bestehen hier keine formalen Trennungen zwischen Netz, Vertrieb und Betriebstechnik. Dies führt zu eng verflochtenen Prozessen, aber auch zu besonderen Herausforderungen bei der Regelungszuordnung, Nachweisführung und Verantwortlichkeitsklärung. Hinweis: Gas-, Wasser- oder Wärmenetze sind zwar häufig Teil des organisatorischen Gesamtverbunds, werden in dieser Analyse jedoch nicht berücksichtigt.

3.1 Problemstellung

Das integrierte Stadtwerk steht exemplarisch für viele Versorgungsunternehmen, die eine Vielzahl technischer, organisatorischer und rechtlicher Anforderungen erfüllen müssen, ohne jedoch über die formalen Ressourcen und Zuständigkeiten großer Konzerne zu verfügen. In Deutschland gibt es rund 1.000 Stadtwerke, die als kommunale Energieversorgungsunternehmen tätig sind. Mit Stand Mai 2025 sind beim Bundesamt für Sicherheit in der Informationstechnik (BSI) jedoch lediglich 301 Betreiber Kritischer Infrastrukturen (KRITIS) im Sektor Energie registriert, darunter auch Übertragungsnetzbetreiber, Verteilnetzbetreiber sowie größere Erzeugungsunternehmen und Aggregatoren. Durch die aktuellen Gesetzesnovellen ist zu erwarten, dass künftig deutlich mehr Stadtwerke, insbesondere solche, die bislang nicht als KRITIS-Betreiber eingestuft sind, verpflichtet sein werden, KRITIS-nahe IT-Sicherheits- und Organisationsstandards zu erfüllen.

Damit geraten insbesondere kleinere und mittelgroße Stadtwerke unter erheblichen Anpassungsdruck, da ihnen im Vergleich zu großen Konzernen oft die spezialisierten Ressourcen für IT-Sicherheit, Compliance und Governance fehlen.

Die gleichzeitige Koexistenz unterschiedlicher Systemgenerationen (Alt-OT und moderne IT), begrenzte Personalressourcen, sektorale Anforderungen sowie uneinheitliche Prüfregime führen zu einer operativen Überforderung bei der geordneten Sicherheits- und Resilienzumsetzung. Im Zentrum des Handelns sollte hier jedoch nicht nur der Schutz einzelner Systeme stehen, sondern die Frage, wie Stadtwerke ihre Resilienz gegenüber komplexen, systemischen Risiken aufbauen können.

3.1.1 Versorgungsaufgabe und Betriebsverantwortung

Das betrachtete integrierte Stadtwerk übernimmt eine Vielzahl zentraler Aufgaben innerhalb der lokalen Stromversorgung. Als Betreiber von Stromverteilnetzen verantwortet es die physische Energieverteilung ebenso wie die kontinuierliche Netzführung auf Verteilnetzebene, einschließlich Wartung und Störfallmanagement, Netzentwicklung und Netzführung, sowie den Vertrieb und Energiehandel. Darüber hinaus ist es für die Umsetzung der regulatorischen Anforderungen entlang der Marktkommunikation und der Netzzugangsprozesse sowie auch für den Messstellenbetrieb als grundzuständiger Messstellenbetreiber (gMSB) zuständig.

Einordnung nach BSI-KritisV

Obwohl das Stadtwerk vielfältige systemrelevante Aufgaben im Bereich Stromnetz, Messwesen, Vertrieb und Erzeugung übernimmt, liegt es in seiner konkreten Ausprägung unterhalb der kritischen Schwellenwerte gemäß BSI-KritisV:

Im Bereich Stromverteilnetz werden weniger als 100.000 Letztverbraucher versorgt, die installierte Erzeugungsleistung liegt unterhalb von 420 MW brutto.

Auf dieser Grundlage wird das Stadtwerk nicht als KRITIS im engeren Sinne klassifiziert.

3.1.2 Systemlandschaft

Die technische Systemlandschaft des integrierten Stadtwerks umfasst eine Vielzahl unterschiedlicher Komponenten, die entlang der gesamten energiewirtschaftlichen Wertschöpfungskette angeordnet sind. Sie bilden die infrastrukturelle Grundlage für den sicheren Netzbetrieb, die Marktprozesse, den Vertrieb und den Messstellenbetrieb. Eine vereinfachte Systemübersicht ist in Tabelle 6 dargestellt.

Im Bereich der Netzführung kommen klassische OT-Systeme zum Einsatz, darunter Netzleittechnik (SCADA), Fernwirktechnik, Remote Terminal Units (RTU), speicherprogrammierbare Steuerungen (SPS) und digitale Netzmodelle. Diese Systeme dienen der Steuerung und Überwachung der Stromverteilnetze sowie der Umsetzung netzbezogener Maßnahmen. Die Wartung und Störfallbearbeitung werden durch digitale Entstörsysteme, mobile Meldeplattformen, Alarmserver und Instandhaltungsmanagementsysteme unterstützt, die zunehmend mit IT-gestützten Planungs- und Rückmeldetools gekoppelt sind. Die Netzentwicklung und Netzplanung erfolgen auf Basis spezialisierter Engineering-Software wie Netzberechnungsprogrammen, Geoinformationssystemen (GIS-Systemen) und Asset-Management-Lösungen. Diese Systeme ermöglichen die strategische Entwicklung der Infrastruktur sowie die langfristige

Integration neuer Anlagen und Technologien. Im Bereich Messwesen nutzt das Stadtwerk Systeme zur Administration intelligenter Messsysteme, darunter GWA, CLS-Managementplattformen und externe Meter Data Management Systems (MDMS). Diese Systeme sind sowohl im OT- als auch im IT-Bereich verortet und spielen eine zentrale Rolle für die sichere Datenerhebung und -übertragung.

	Typische Systeme/Komponenten	Verortung (OT/IT)
Netzführung (Strom)	Netzleitsystem (SCADA), RTU, SPS, Fernwirktechnik, Netzschutz	OT
Wartung & Störfall-management	Instandhaltungs- und Entstörsysteme, mobile Rückmelde-Apps, Melde-wege, Alarmserver, Netzmeldemanagement	OT/IT
Netzentwicklung & Netzplanung	Netzberechnungstools, GIS-Systeme, Asset Management, Planungs-software	IT
Messwesen (gMSB)	GWA-Backend, CLS-Management, SMGW-Administration, externes MDMS, Geräteverwaltung, Zertifikatsmanagement	OT/IT
Marktkommunikation	AS4-Kommunikation, B2B-Gateways, Formatprüfer, BDEW-Web Appli-cation Programming Interface (API)	IT
Vertrieb	CRM-Systeme, Tarifmodellierung, Vertragsmanagement, Kundenportale, Self-Service-Plattformen	IT
Energiehandel & Bilan-zierung	ETRM-Systeme, Börsenanbindung (EPEX/EEX), Bilanzkreissystem, Prognosetools, Redispatch 2.0, Fahrplanmanagementsysteme	IT
Abrechnung & Fakturierung	SAP IS-U (oder gleichwertig), Rechnungsstellung, Zahlungsverkehr, Marktpreisverarbeitung, Verbrauchsdatenmanagement	IT
Datenmanagement & Analyse	Monitoring-Lösungen, cloudbasierte Auswertung, KPI-Dashboards, Performance-Analysen	IT
Schnittstellen & Integration	Middleware, Protokollumsetzer, Segmentierungs-Firewalls, Gateways, API-Plattformen	OT/IT

Tabelle 6: Systemlandschaft des integrierten Stadtwerks gegliedert nach Aufgabenbereichen und Systemtypen

Die Marktkommunikation stützt sich auf IT-Systeme wie AS4-Server, B2B-Gateways, Formatprüfer und weitere Komponenten zur Umsetzung regulatorischer Kommunikationsprozesse im Rahmen der Geschäftsprozesse zur Kundenbelieferung mit Elektrizität (GPKE) sowie MaBiS Marktregeln für die Durchführung der Bilanzkreisabrechnung Strom. Diese Systeme sind in standardisierte Marktrollen eingebettet und technisch eng mit den Mess-, Abrechnungs- und ERP-Systemen (Enterprise Resource Planning) verknüpft. Im Vertrieb kommen Customer-Relationship-Management-Systeme (CRM), Tarif- und Vertragsverwaltungsplattformen sowie Kundenportale zum Einsatz. Sie ermöglichen die zielgerichtete Kundeninteraktion und bilden die Basis für energiewirtschaftliche Geschäftsmodelle. Die Energiebeschaffung und Bilanzierung erfolgen auf Basis von Energiehandels- und Portfoliomanagementsystemen (Enterprise Resource Planning, ETRM), Prognosewerkzeugen,

Bilanzkreismodulen und Fahrplanmanagementsystemen. Sie sind vielfach an Börsenschnittstellen (z. B. European Power Exchange (EPEX) und European Energy Exchange (EEX)) sowie an Redispatch-Systeme gekoppelt und bilden eine zentrale Säule der wirtschaftlichen Energieversorgung. Im Bereich Abrechnung und Fakturierung werden Systeme wie SAP Industry Solution for Utilities (IS-U) oder vergleichbare Plattformen eingesetzt, die Tariflogik, Rechnungsstellung, Zahlungsabwicklung und Vertragsverarbeitung integriert abbilden. Sie sind mit Datenquellen aus Messwesen, Vertrieb und Marktkommunikation verbunden. Ergänzt wird die Systemlandschaft durch verschiedene Lösungen zur Datenverarbeitung, Analyse und Visualisierung, etwa cloudbasierte Monitoring-Plattformen, Performance-Kennzahlen, Zustandsbewertung oder Prognosewerkzeuge. Schließlich sind Schnittstellen-, Übersetzungs- und Segmentierungskomponenten Bestandteil der Infrastruktur. Dazu zählen Middleware, Gateways, Protokollumsetzer und Segmentierungs-Firewalls. Sie sind erforderlich, um Systeme unterschiedlicher Generationen, Hersteller und Sicherheitsniveaus miteinander zu verbinden.

Diese Systemlandschaft ist funktional eng verflochten, technologisch heterogen und vielfach historisch gewachsen. Daraus ergeben sich eine Vielzahl potenzieller Schnittstellenrisiken sowie komplexe Betriebs- und Absicherungserfordernisse. Die spezifische Ausprägung der hybriden Architektur sowie die sich daraus ergebenden Herausforderungen werden im folgenden Abschnitt näher analysiert.

3.1.3 Hybride Infrastruktur und technische Übergangszonen

Die Systemlandschaft des integrierten Stadtwerks ist nicht nur vielfältig, sondern strukturell hybrid. Sie setzt sich aus Komponenten unterschiedlicher technischer Generationen und mit verschiedenen Kommunikationsprotokollen und Sicherheitsparadigmen zusammen. Diese Hybridität betrifft sowohl den vertikalen Technologie-Stack, von der Feldebene bis zur Managementebene, als auch die horizontale Integration verschiedener Systeme innerhalb einzelner Prozessketten.

Klassische OT-Systeme wie RTUs, SPS und serielle Fernwirktechnik basieren auf stabilen, aber häufig langjährig betriebenen Infrastrukturen mit begrenzter Update-Fähigkeit. Sie wurden ursprünglich für physische Robustheit und deterministische Prozessführung konzipiert, nicht jedoch für moderne Cybersicherheitsanforderungen. Demgegenüber stehen zunehmend eingesetzte IP-basierte (Internet Protocol) IT-Systeme, etwa für Gateway-Administration, Prognoseberechnungen oder Marktkommunikation, mit höheren Update-Frequenzen, kürzeren Produktlebenszyklen und cloudnahen Integrationsmodellen.

Die Verbindung dieser Systeme erfolgt über sogenannte technische Übergangszonen: Middleware, Gateways, Protokollkonverter und Segmentierungskomponenten sorgen dafür, dass Datenflüsse zwischen heterogenen Systemen möglich sind, etwa zwischen einer SPS und einem AS4-Kommunikationsserver oder zwischen einem CLS-Modul und einem ERP-System. Diese Übergänge sind funktional notwendig, stellen aber auch sicherheitskritische Knoten dar.

Typische Merkmale und Herausforderungen hybrider Infrastrukturen sind:

Inkompatible Lebenszyklen: Während OT-Komponenten auf jahrzehntelangen Betrieb ausgelegt sind, erfordern IT-Systeme laufende Updates und Nachpflege, was zu Wartungsbrüchen führt.

Heterogene Protokolle und Datenformate: Proprietäre OT-Protokolle treffen auf moderne Web- und API-basierte Kommunikationsstandards, was Integrationsaufwand und Fehleranfälligkeit erhöht.

Segmentierungsdefizite: In vielen Bestandsnetzen existiert keine konsequente logische oder physische Trennung zwischen IT- und OT-Bereichen, was die Angriffsfläche deutlich vergrößert.

Kooperationsabhängigkeit: Die Pflege hybrider Umgebungen erfordert die enge Zusammenarbeit von unterschiedlichen Herstellern, Systemintegratoren und externen Dienstleistern mit teils unklarer Zuständigkeit bei Sicherheits- oder Update-Fragen.

Schwierige Zertifizierbarkeit: Komplexe und gemischte Systemlandschaften lassen sich nur schwer standardkonform absichern, insbesondere bei Kombinationen aus veralteter OT und neuen, cloudbasierten IT-Komponenten.

Besonders herausfordernd ist, dass sicherheitsrelevante Funktionen oftmals prozess- und systemübergreifend implementiert sind. Einfache Steuerbefehle oder Datenübertragungen durchlaufen verschiedene Schichten, ohne dass ihre gesamtheitliche Absicherung durch eine einheitliche Architektur gewährleistet ist. Dies betrifft sowohl operative Netzprozesse als auch Marktkommunikation, Redispatch oder CLS-Steuerung.

Diese hybriden Infrastrukturen erfordern daher herausfordernde Ansätze im technischen und organisatorischen Risikomanagement, jenseits klassischer ISMS-Logiken. Im nächsten Abschnitt wird daher die regulatorische Einbettung dieser Herausforderungen näher betrachtet.

3.1.4 Regulatorische Anforderungen an unser Stadtwerk

Auch wenn das betrachtete Stadtwerk in seiner konkreten Ausprägung nicht unter die formale Einstufung als KRITIS im Sinne der BSI-KritisV fällt, unterliegt es dennoch einer Vielzahl von regulatorischen Anforderungen. Diese ergeben sich aus sektorspezifischen wie auch übergreifenden Rechtsvorgaben und betreffen sowohl die technische Absicherung als auch die organisatorische Ausgestaltung sicherheitsrelevanter Prozesse.

Energiewirtschaftsgesetz (EnWG): Gemäß § 11 EnWG sind alle Betreiber von Energieversorgungsnetzen und Energieanlagen, unabhängig von ihrer Größe oder KRITIS-Einstufung, verpflichtet, angemessene technische Vorkehrungen zum Schutz ihrer Telekommunikations- und IT-Systeme zu treffen. Diese gesetzliche Grundlage wurde durch zwei separate IT-Sicherheitskataloge der BNetzA konkretisiert:

- IT-Sicherheitskatalog für Netzbetreiber (seit 2015): verpflichtend für alle Strom- und Gasnetzbetreiber
- IT-Sicherheitskatalog für Energieanlagenbetreiber (seit 2021): gilt für Betreiber von Erzeugungsanlagen, insbesondere bei Redispatch-Beteiligung oder Marktsteuerung

Beide Sicherheitskataloge gelten unabhängig von der sogenannten De-minimis-Schwelle (§ 7a EnWG) und entfalten damit auch für kleinere Stadtwerke mit integrierter Systemarchitektur unmittelbare Wirkung. Die De-minimis-Schwelle in § 7a EnWG bezieht sich auf die Ausnahme von den Entflechtungsanforderungen für vertikal integrierte Energieversorgungsunternehmen (also Unternehmen, die sowohl Netzbetrieb als auch Vertrieb betreiben) mit weniger als 100.000 angeschlossenen Kunden (direkt oder indirekt).

Zusätzlich zu den IT-Sicherheitskatalogen ist das Stadtwerk als Verteilnetzbetreiber verpflichtet, steuerbare Verbrauchseinrichtungen gemäß § 14a EnWG in das Netz zu integrieren. Dies erfordert die Einrichtung sicherer Steuerungspfade, insbesondere über die CLS-Kanäle des intelligenten Messsystems. Die Festlegungen der BNetzA (Az. BK6-22-300) konkretisieren hierzu technische, organisatorische und sicherheitsrelevante Anforderungen, die unmittelbar in die Systemlandschaft und das ISMS des Netzbetreibers einzubinden sind (BNetzA, 2022c).

Messstellenbetriebsgesetz (MsbG): Als grundzuständiger Messstellenbetreiber (gMSB) ist das Stadtwerk ebenfalls an die Vorgaben des Messstellenbetriebsgesetzes gebunden. Hieraus ergeben sich insbesondere Pflichten im Bereich des sicheren Betriebs intelligenter Messsysteme, einschließlich GWA-Backend, CLS-Management und Nutzung zertifizierter IT-Komponenten. Die relevanten technischen Anforderungen, Schutzprofile und BSI-Richtlinien (insbesondere TR-03109) sind in Kapitel 2.2 zusammengefasst.

IT-Sicherheitsgesetz 2.0 / BSI-Gesetz (BSIG): Auch wenn keine formale KRITIS-Zuordnung vorliegt, entfalten ausgewählte Pflichten aus dem IT-Sicherheitsgesetz 2.0 und dem BSIG faktisch Wirkung. Dies betrifft insbesondere Anforderungen an die Risikobewertung, die Meldebereitschaft bei Sicherheitsvorfällen, Maßnahmen zum Schutz kritischer Systeme und die Orientierung am „Stand der Technik“. Weitere Ausführungen zu strukturellen Überschneidungen mit den Sicherheitskatalogen sowie zur Rolle des BSI als Aufsichtsinstanz finden sich in Kapitel 2.4.

Auf Basis dieser Ausgangslage lassen sich typische Spannungsfelder identifizieren, die im integrierten Stadtwerk immer wieder auftreten, sowohl in technischer als auch in organisatorischer und regulatorischer Hinsicht.

3.2 Systemische Spannungsfelder im integrierten Betrieb

Das Zusammenspiel technischer Komponenten, organisatorischer Verantwortung und regulatorischer Vorgaben führt im integrierten Stadtwerk zu einer Vielzahl struktureller Spannungsfelder. Diese ergeben sich nicht primär aus isolierten Einzelrisiken, sondern aus den systemischen Wechselwirkungen zwischen unterschiedlichen Systemgenerationen, Betriebslogiken und Steuerungsebenen. Besonders herausfordernd ist dabei die gleichzeitige Beherrschung von Alt-OT, modernisierter IT-Infrastruktur, Marktkommunikation und intelligentem Messwesen.

Schnittstellenverantwortung am Beispiel des § 14a EnWG

Ein besonders anschauliches Beispiel für die Herausforderungen technischer und organisatorischer Schnittstellenverantwortung liefert die Umsetzung des § 14a EnWG. Zwar ist der Netzbetreiber gesetzlich verpflichtet, steuerbare Verbrauchseinrichtungen über das intelligente Messsystem in das Stromnetz zu integrieren, doch erfolgt die technische Steuerung typischerweise über CLS-Komponenten, die organisatorisch und betrieblich dem grundzuständigen Messstellenbetreiber zugeordnet sind.

Diese arbeitsteilige Umsetzung erzeugt komplexe Schnittstellen zwischen Netzbetreiber, Gateway-Administrator (GWA) und externen Dienstleistern. Dabei ist häufig weder die technische Zuständigkeit eindeutig geregelt noch die sicherheitsbezogene Verantwortung konsistent zugewiesen.

In ihrer Konsultation zur Neufassung der IT-Sicherheitskataloge (BNetzA, 2025, Zeilen 146-148) greift die BNetzA diese Problematik ausdrücklich auf. Sie stellt die Frage, ob die bestehende Trennung zwischen Marktrollen und Systemgrenzen überhaupt hinreichend eindeutig ist. Diese Konsultationsfrage unterstreicht die anhaltende Ambiguität in der Praxis und verweist auf den grundsätzlichen Klärungsbedarf hinsichtlich einer übergreifenden Steuerungsverantwortung in hybriden Versorgungsarchitekturen.

Diese Schnittstellenrisiken wirken in hybriden Infrastrukturen besonders gravierend, da sie technische und organisatorische Koordinationsbedarfe zugleich betreffen. In vielen integrierten Stadtwerken existiert bislang keine explizit institutionalisierte Gesamtverantwortung, die sicherheitsrelevante Funktionen übergreifend systemisch steuert. Stattdessen sind Rollen und Zuständigkeiten entlang der Wertschöpfung

funktional verteilt, etwa zwischen Netzbetrieb, Gateway-Administration und Marktkommunikation, jedoch nicht durchgängig mit einem gemeinsamen Sicherheits- oder Risikomanagement verknüpft.

Diese strukturelle Fragmentierung erschwert die konsolidierte Risikoanalyse und behindert im Ereignisfall ein abgestimmtes Incident Management. Auch im Regelbetrieb zeigen sich Auswirkungen: So fehlt häufig eine zentrale Instanz, die Systemänderungen, etwa bei Updates oder Integrationsprojekten, im Hinblick auf sicherheitsrelevante Wechselwirkungen entlang der Prozesskette beurteilt.

3.2.1 Lebenszykluskonflikte und Modernisierungsasymmetrien

Ein wesentliches Spannungsfeld im Betrieb integrierter Stadtwerke liegt in den strukturellen Unterschieden der Lebenszyklen von OT- und IT-Systemen. Während klassische OT-Komponenten auf einen jahrzehntelangen Betrieb ausgelegt sind, unterliegen IT-Systeme, etwa für Marktkommunikation oder Abrechnung, deutlich kürzeren Innovationszyklen von drei bis sieben Jahren. Daraus entstehen sogenannte Modernisierungsasymmetrien, die sich auf Betrieb, Wartung und Sicherheit der Gesamtinfrastruktur spürbar auswirken.

Wartungs- und Update-Brüche zählen dabei zu den unmittelbarsten Folgen: Während IT-Systeme kontinuierlich aktualisiert werden (müssen), fehlen bei vielen OT-Komponenten die technischen, organisatorischen oder regulatorischen Voraussetzungen für regelmäßige Updates. Das betrifft etwa fehlende Herstellerunterstützung („End of Life“-Status), eingeschränkte Kompatibilität mit aktuellen Sicherheits-Patches oder restriktive Fernwartbarkeit. Diese Diskrepanz führt zu Brüchen in der gemeinsamen Patch- und Sicherheitsstrategie und erschwert die Integration in ganzheitliche Managementsysteme nach ISO 27001.

Hinzu kommen inkompatible Release-Zyklen und divergierende Betriebslogiken: IT-Komponenten folgen häufig standardisierten ITIL-Prozessen (Information Technology Infrastructure Library) und sind auf agile Anpassung ausgelegt, während OT-Systeme stabilitätsorientiert betrieben und selten verändert werden. Die gleichzeitige Steuerung solcher heterogener Systemumgebungen stellt erhebliche Anforderungen an Change-, Konfigurations- und Notfallprozesse. Besonders problematisch wird dies bei Systemkopplungen entlang der Prozesskette, etwa zwischen einem ERP-System, einem extern betriebenen GWA-Backend und einer lokalen Netzleitstelle. Hier treffen oft uneinheitliche Dokumentationsstandards, Testverfahren und Zuständigkeiten aufeinander.

Verstärkt wird diese Herausforderung durch verdeckte Interdependenzen: Viele Altsysteme wurden über Jahre hinweg mit neuen Komponenten gekoppelt, ohne dass diese Übergänge systematisch dokumentiert oder vollständig verstanden wurden. Derartige Kopplungseffekte, etwa durch Middleware, Emulationslayer oder individuell entwickelte Schnittstellen, können dazu führen, dass Änderungen an einem Teilsystem unbeabsichtigte Auswirkungen auf andere Komponenten haben, etwa Dateninkonsistenzen, Übertragungsfehler oder Störungen im Automatikbetrieb. Solche Risiken sind schwer zu erkennen und noch schwerer zu beheben, da sie oft unterhalb der formalen Zuständigkeitsschwellen operieren.

Ein weiteres strukturelles Risiko ergibt sich durch die anhaltende Praxis temporärer Überbrückungslösungen, die sich bei vielen Versorgern zu dauerhaften Betriebsbestandteilen entwickelt haben. Protokollkonverter, manuelle Importe, ungesicherte Übergabepunkte oder Einzellösungen zur Prozessintegration werden mangels Ressourcen oder Alternativen dauerhaft betrieben, jedoch meist ohne systematische Validierung und Risikobewertung oder regelmäßige Testzyklen. Dies führt zu einer schleichenden „technischen Verschuldung“ (engl. Technical Debt), die sowohl Betriebsrisiken als auch Angriffsflächen erhöht. „Technical Debt“ beschreibt metaphorisch die zukünftigen Kosten, die entstehen,

wenn man jetzt eine schnelle, aber nicht ideale Lösung wählt, anstatt einen besseren, aber zeitaufwendigeren Ansatz zu verfolgen.

Nicht zuletzt stellt das sogenannte Sicherheitsparadoxon bei Altsystemen eine zentrale Herausforderung dar. Während diese Systeme durch ihre lange Nutzung vermeintlich robust erscheinen, erfüllen sie häufig keine heutigen Sicherheitsanforderungen. Die häufig genutzte Strategie einer vermeintlichen „Security by Obscurity“, also das Vertrauen darauf, dass veraltete Systeme durch Intransparenz geschützt sind, erweist sich im Lichte moderner Angriffsformen zunehmend als unzureichend. Gleichzeitig ist eine Absicherung durch aktuelle Standards oft nur eingeschränkt möglich oder wirtschaftlich nicht darstellbar.

KETEL & Co.: Wenn moderne Sicherheit auf alte Protokolle trifft

In vielen Stadtwerken kommunizieren OT-Komponenten wie SCADA-Systeme über herstellerspezifisch angepasste Protokolle (z. B. KETEL). Diese wurden nie für heutige Sicherheitsanforderungen entwickelt und nicht offen dokumentiert. Moderne Sicherheitssysteme wie Anomalieerkennung oder Deep Packet Inspection (DPI) stoßen hier an Grenzen:

- Kommunikationsinhalte lassen sich kaum auslesen oder semantisch interpretieren.
- Protokollvielfalt und Intransparenz verhindern eine einheitliche Analyse.
- Schwachstellen bleiben unerkannt, Forensik und Monitoring sind lückenhaft.

Diese Intransparenz suggeriert trügerisch Sicherheit („Security by Obscurity“), blockiert aber in Wahrheit die Integration in übergreifende Schutzkonzepte. Zugleich zeigt sich ein klassischer Lebenszykluskonflikt: Neue Sicherheitstechnologien treffen auf veraltete, schwer migrierbare Infrastrukturen, die sich modernen Anforderungen entziehen. Ohne Offenlegung und Standardisierung bleibt ein integrativer Sicherheitsansatz kaum realisierbar.

3.2.2 Fragmentierte Prüflogiken und regulatorische Überschneidungen

Im integrierten Stadtwerk greifen unterschiedliche regulatorische Anforderungen ineinander (vgl. Kapitel 2.2). Hinzu kommen spezifische Vorgaben der BNetzA, etwa die IT-Sicherheitskataloge für Netzbetreiber und Energieanlagen sowie Vorgaben zur Marktkommunikation. Diese Vorgaben richten sich jedoch jeweils an unterschiedliche Marktrollen, Systemtypen oder Funktionseinheiten, ohne auf ihre technologische oder organisatorische Verzahnung im integrierten Betrieb Rücksicht zu nehmen.

Besonders problematisch ist dabei, dass die zugehörigen Prüf- und Zertifizierungsregime stark divergieren: Während IT-Systeme typischerweise durch ISO-Audits oder IT-Grundschutz-Prüfungen bewertet werden, gelten für OT-Systeme teilweise Technische Richtlinien, Branchenspezifische Sicherheitsstandards oder Herstellerzertifikate. Für hybride Prozesse, wie sie in integrierten Stadtwerken typisch sind (z. B. bei CLS-Steuerung oder Redispatch 2.0), existieren bislang keine abgestimmten Prüfkonzepte oder systemübergreifenden Zertifizierungsmodelle.

Hinzu kommt, dass viele Prüfvorgaben stark rollenbasiert formuliert sind, etwa für den gMSB, den Netzbetreiber oder die Betreiber einer Energieanlage. In integrierten Organisationen fallen diese Rollen jedoch oftmals in eine gemeinsame Verantwortungseinheit, wodurch sich Mehrfachprüfungen, konkurrierende Anforderungen und Inkonsistenzen in der Umsetzung ergeben. Gleichzeitig bleiben kritische Schnittstellen,

etwa zwischen Netzführung, GWA-Backend und Marktkommunikation, außerhalb des formalen Prüfrahmens.

Eine durchgängige Validierung über Systemgrenzen hinweg, etwa zwischen Gateway-Administration, Marktkommunikationsservern und Netzleittechnik, gestaltet sich in der Praxis äußerst anspruchsvoll. Die Herausforderung resultiert weniger aus einem prinzipiellen technischen Unvermögen, als vielmehr aus der fehlenden methodischen Verzahnung zwischen unterschiedlichen Prüfregimen, dem Nebeneinander inkompatibler Standards sowie uneinheitlichen Zuständigkeiten innerhalb der Organisation. In der Folge bleiben sicherheitsrelevante Übergänge häufig außerhalb formalisierter Auditpfade, mit der Konsequenz, dass vorhandene Schutzmaßnahmen zwar jeweils für sich geprüft und zertifiziert sein mögen, ihre systemübergreifende Wirksamkeit jedoch schwer nachweisbar ist.

Redispatch 2.0 im integrierten Stadtwerk als Prüf- und Governance-Herausforderung

Im Rahmen von Redispatch 2.0 übernimmt das integrierte Stadtwerk typischerweise mehrere Rollen: Es agiert nicht nur als Verteilnetzbetreiber (VNB), sondern häufig auch als Einsatzverantwortlicher (EIV), Betreiber technischer Ressourcen (BTR) und Bilanzkreisverantwortlicher (BKV). Die jeweiligen Aufgaben umfassen Prognosebereitstellung, Maßnahmenplanung, Fahrplanabgleich und die operative Umsetzung netzstützender Eingriffe.

Besonders herausfordernd ist dabei die Abbildung sicherheitsrelevanter Funktionen, da zentrale Steuerungspflichten über mehrere Systemgrenzen hinweg erfolgen: von der Erzeugungsanlage über das Netzleitsystem bis hin zum Marktkommunikationsserver und den Redispatch-Schnittstellen.

Trotz dieser kritischen Interdependenzen bleiben viele Prüf- und Sicherheitsvorgaben auf organisationsinterne Prozesse beschränkt. Die notwendige Abstimmung mit überlagertem Netzbetreiber, Übertragungsnetzbetreiber, externen Einsatzverantwortlichen oder Vermarktern ist häufig weder methodisch vorgesehen noch auditierbar.

3.2.3 Abhängigkeiten von externen Dienstleistern und Herstellern

In integrierten Stadtwerken beruhen zentrale IT- und OT-Funktionalitäten zunehmend auf der Mitwirkung externer Dienstleister, Systemintegratoren und Hersteller. Diese Kooperationen sind aufgrund der hohen Spezialisierung vieler Systemkomponenten und begrenzter interner Ressourcen meist alternativlos, bringen jedoch erhebliche sicherheitsrelevante Abhängigkeiten mit sich.

Ein zentrales Risiko liegt in der begrenzten Transparenz hinsichtlich sicherheitsrelevanter Betriebsprozesse Dritter. Insbesondere in ausgelagerten Betriebsmodellen fehlt häufig die vollständige Einsicht in Update-Zyklen, Patch-Management, Systemkonfigurationen oder Nutzerrechteverwaltung. Die technische Verantwortung für einen Prozess liegt dann außerhalb der eigenen Governance-Reichweite, während die formale Betreiberverantwortung bestehen bleibt. Dies erschwert eine durchgängige Risikoanalyse sowie die Nachweisführung im Rahmen von Audits oder Zertifizierungen.

Besonders kritisch sind Fernwartungsschnittstellen, über die externe Anbieter privilegierte Zugriffe auf sensible OT- oder IT-Komponenten erhalten. In der Praxis erfolgt dieser Zugriff häufig über unzureichend geschützte VPN-Verbindungen oder proprietäre Fernwartungsprotokolle, ohne systematische Protokollierung, Zugriffskontrolle oder Integritätsüberwachung. Der Schutz solcher Übergänge erfordert dedizierte

Sicherheitsmaßnahmen wie Jump Hosts, PAM-Systeme (Privileged Access Management) oder durchgehendes Session-Monitoring, die jedoch bislang selten flächendeckend implementiert sind.

Ein weiterer strategischer Risikofaktor besteht in technologischen Lock-in-Effekten. Viele eingesetzte Komponenten basieren auf proprietären Datenformaten, geschlossenen Schnittstellen und exklusiven Herstellerzertifikaten. Dies erschwert sowohl die Interoperabilität mit anderen Systemen als auch eine flexible Reaktion auf Sicherheitsvorfälle, etwa durch Wechsel der Anbieter oder kurzfristige Migrationen. Nicht selten sind auch Support- und Wartungsleistungen an exklusive Betriebsvereinbarungen gebunden, die die Abhängigkeit zusätzlich verstärken.

Mehrere Anbieter, keine Klarheit, Sicherheitsrisiko Schnittstellenverantwortung

Die Marktkommunikation in der Energiewirtschaft erfolgt zunehmend über komplexe Systemverbünde: Eine AS4-Kommunikationslösung wird von Hersteller A bereitgestellt, die zugehörige Server- und Netzwerkinfrastruktur betreibt ein externer Dienstleister B, während weitere Hersteller zusätzliche Anwendungen liefern, die auf den Kommunikationsserver zugreifen. Diese arbeitsteilige Struktur bringt funktionale Effizienz, jedoch auch erhebliche Risiken im Bereich der Sicherheitsverantwortung mit sich.

Im Fehlerfall erweist sich die Zuordnung von Ursachen als besonders herausfordernd: Unklare Zuständigkeiten, inkompatible Diagnosewerkzeuge und fehlende Schnittstellenstandards erschweren eine systematische Fehlerortung. Der Einsatz herstellerspezifischer Tools verhindert häufig eine durchgängige Protokollanalyse. Zudem liegt der operative Zugriff auf kritische Komponenten (z. B. Firewall-Konfigurationen, Zertifikatsverwaltung oder AS4-Gateways) oft außerhalb der eigenen Governance-Reichweite des Betreibers.

Diese fragmentierte Struktur untergräbt sowohl die Sicherheitsüberwachung als auch die Nachweisführung gegenüber Dritten. Ohne verbindliche Prozessbeschreibungen, eine zentrale Dokumentation und standardisierte Kontrollmechanismen bleibt die Resilienz solcher Mehranbieter-Konstellationen begrenzt, insbesondere dort, wo systemübergreifende Incident-Response- oder Monitoring-Prozesse nicht etabliert sind.

Auch auf der Ebene der regulatorischen Nachweisführung bestehen Herausforderungen: Viele externe Partner unterliegen nicht denselben regulatorischen Anforderungen wie der Betreiber selbst. Gerade bei Subunternehmerketten oder Cloud-Anbietern besteht das Risiko, dass sicherheitsrelevante Maßnahmen zwar formal zugesagt, aber nicht überprüfbar oder auditierbar sind. Dies untergräbt die ganzheitliche Risikotransparenz des Stadtwerks und kann im Störungs- oder Prüfungsfall zu Unsicherheiten führen.

Diese strukturellen Risiken zeigen, dass der reine auf einem Service Level Agreement (SLA) basierende Steuerungsansatz nicht ausreicht, um die Sicherheit ausgelagerter Betriebsfunktionen zu gewährleisten. Ein SLA, also eine Dienstleistungsvereinbarung oder Dienstgütevereinbarung, ist ein Vertrag zwischen einem Dienstleister und einem Kunden, der die zu erbringenden Dienstleistungen, ihren Umfang und das zu erwartende Leistungsniveau genau festlegt. In der Regel werden Reaktionszeiten für definierte Anwendungsfälle (z. B. Behebung von Störungen oder Fehlern) minutengenau festgelegt. Vielmehr bedarf es eines verbindlichen und standardisierten Dienstleister-Managements, das sowohl technische als auch vertragliche Kontrollmechanismen systematisch verankert.

3.2.4 Governance-Kohärenz und Managementintegration

Im integrierten Stadtwerk ist die sicherheitsbezogene Steuerung meist auf mehrere Ebenen verteilt. Die Koordination dieser Ebenen gestaltet sich jedoch häufig komplex, insbesondere weil sicherheitsrelevante Anforderungen nicht konsistent in die übergreifende Unternehmenssteuerung integriert sind.

In vielen Fällen bestehen funktional getrennte Verantwortlichkeiten für Informationssicherheit, Betriebssicherheit, Datenschutz, Notfallmanagement und technische Compliance. Sie werden innerhalb einzelner Fachbereiche gewissenhaft wahrgenommen, doch fehlt es mitunter an einer verbindlichen, strukturell verankerten Gesamtkoordination. Gerade an den Schnittstellen zwischen Netzbetrieb, Messwesen, Marktkommunikation und Energieanlagenbetrieb entstehen dadurch Interpretationsspielräume, beispielsweise im Hinblick auf Zuständigkeiten im Störfall oder bei der Umsetzung regulatorischer Vorgaben.

Hinzu kommt, dass sicherheitsbezogene Aufgaben nicht in allen Stadtwerken systematisch mit der strategischen Steuerung verknüpft sind. Zwar existieren häufig projektbezogene Umsetzungen von ISMS-Strukturen oder Sicherheitskonzepten, doch ihre Einbindung in Unternehmensziele, Gremienentscheidungen oder Investitionsplanungen erfolgt vielfach selektiv. Sicherheitsbudgets werden in diesem Zusammenhang oft als Kostenblöcke betrachtet, nicht jedoch als Bestandteil langfristiger Wertschöpfungs- und Resilienzstrategien.

Auch die Integration in bestehende Governance- und Managementsysteme ist ausbaufähig. Während in anderen Bereichen klare Prozesse, Rollen und Berichtslinien etabliert sind, zeigt sich bei der Steuerung hybrider Infrastrukturen oft eine fragmentierte Praxis. Eine übergreifende Governance-Struktur, die technische Sicherheitsmaßnahmen mit betrieblicher Kontinuität, IT-/OT-Integration und strategischer Unternehmensplanung verzahnt, ist noch nicht flächendeckend etabliert.

Ein weiterer Aspekt betrifft die Entwicklung einer Sicherheitskultur: Maßnahmen zur Awareness und Schulung sind zwar vereinzelt vorhanden, doch fehlen vielerorts strukturierte Programme, um ein organisationsweites Sicherheitsbewusstsein aufzubauen und langfristig zu verankern. Ohne diese Verankerung besteht das Risiko, dass Sicherheitsverantwortung vorwiegend technisch interpretiert und auf einzelne Systeme oder Rollen beschränkt bleibt.

Incident-Beispiel: Fehlende Abstimmung als Governance-Risiko

Von der Fachabteilung wurde ein technisches Monitoring-System zur Überwachung der CLS-Kommunikation eingeführt, um Anomalien im Steuerungspfad frühzeitig zu erkennen. Die Einführung erfolgte jedoch ohne vorherige Abstimmung mit dem ISMS-Team, ohne Einbindung in die zentrale Sicherheitsstrategie und ohne formalisierte Freigabeschleife. Das System nutzt Protokolldaten aus der Kommunikation zwischen GWA-Backend und CLS-Komponenten: ein Bereich, der strengen regulatorischen Vorgaben unterliegt (BSI TR-03109).

Da das Monitoring-System nicht BSI-zertifiziert ist und nicht explizit im Sicherheitskonzept des GWA-Backends berücksichtigt wurde, besteht die Gefahr, dass es gegen geltende regulatorische Anforderungen verstößt und die Nachweisführung im Auditfall erschwert. Auch eine durchgängige Bewertung der Integritäts- und Vertrauensketten ist so nicht möglich. Der Fall verdeutlicht, wie technisch gut gemeinte Einzelinitiativen ohne klare Governance-Anbindung zu regulatorischen Konflikten und Haftungsrisiken führen können.

3.2.5 Bedarf der Übersetzung strategischer Vorgaben in kommunale Strukturen

Ein weiteres strukturelles Spannungsfeld im integrierten Stadtwerk betrifft die Umsetzung strategischer Sicherheitsvorgaben, wie sie etwa durch die NIS2-Richtlinie, das KRITIS-Dachgesetz oder Empfehlungen europäischer Institutionen wie der ENISA formuliert werden. Diese Vorgaben bewegen sich vielfach auf einem hohen Abstraktionsniveau und sind ursprünglich für große Infrastrukturanbieter oder zentrale staatliche Akteure konzipiert. Für kommunale Versorger mit überschaubaren Strukturen, begrenztem Personal und häufig hybriden Betriebsformen ergeben sich daraus erhebliche Umsetzungsprobleme.

Zwischen Brüssel und Berlin – strategische Sicherheit ohne Umsetzungspfad

Ein kommunaler Energieversorger bemüht sich, seine Sicherheitsstrategie an der europäischen NIS2-Richtlinie auszurichten. Doch obwohl die Vorgaben formal beschlossen sind, bleibt unklar, welche konkreten Maßnahmen national gelten werden und welche Schwellenwerte gelten und ab wann.

Die deutsche Umsetzung verteilt sich über mehrere Gesetzesinitiativen, darunter das KRITIS-Dachgesetz, Anpassungen im BSIG und sektorale Regelwerke. Zuständigkeiten sind teils unklar (BMWK, BSI oder BNetzA?), verbindliche Umsetzungsfristen fehlen und begleitende TR oder Orientierungshilfen lassen auf sich warten.

Das Stadtwerk steht vor einem Dilemma: Wer heute Ressourcen investiert, riskiert Fehlsteuerung; wer abwartet, verliert den Anschluss und gerät regulatorisch unter Druck. Diese strategische Lücke erzeugt Stillstand: Weder wird proaktiv investiert noch vorausschauend restrukturiert.

Besonders herausfordernd ist dabei, dass strategische Leitlinien in der Regel keine konkreten Umsetzungspfade bieten. Sie benennen Zielzustände, etwa ein wirksames Risikomanagement, systemübergreifende Incident-Response-Kapazitäten oder robuste Lieferkettensteuerung, lassen jedoch offen, wie sie in mittelständischen Organisationsstrukturen praktisch erreicht werden sollen. Dies zwingt kommunale Energieversorger zu einer eigenständigen „Übersetzungsleistung“: Die allgemeinen Anforderungen müssen in lokale Prozesse, Rollenmodelle und Ressourcenhaushalte überführt und gleichzeitig mit bestehenden nationalen Vorgaben harmonisiert werden.

In vielen integrierten Stadtwerken fehlt für diese anspruchsvolle Transferleistung jedoch eine explizit verankerte Governance-Struktur. Es existieren kaum ressortübergreifende Gremien oder zentrale Steuerungseinheiten, die die Adaption strategischer Anforderungen methodisch begleiten und mit der technischen Realität vor Ort abgleichen. In der Folge verbleiben viele Anforderungen auf der strategischen Metaebene, ohne operational wirksam zu werden. Gleichzeitig entstehen neue Unsicherheiten im Hinblick auf künftige Prüfmaßstäbe, etwa im Rahmen von NIS2 oder dem KRITIS-Dachgesetz.

3.2.6 Resilienzanforderungen – eine wachsende Herausforderung für Stadtwerke

Die systemischen Spannungsfelder in hybriden Versorgungsstrukturen zeigen eindrücklich, dass klassische IT-Sicherheits- und Risikostrukturen nicht mehr ausreichen, um die Anforderungen an einen krisenfesten Netz- und Geschäftsbetrieb zu erfüllen. Mit der erweiterten Fokussierung auf Resilienz, sowohl durch europäische Vorgaben wie die Critical Entities Resilience Directive (CER) (Europäische Union, 2022) als auch durch die angekündigte nationale Umsetzung im KRITIS-Dachgesetz (BSI-KritisV; Bundesrepublik Deutschland, 2023), geraten kommunale Energieversorger zunehmend in die Pflicht, weit über die reine Informationssicherheit hinausgehende Maßnahmen systematisch zu planen und umzusetzen.

Zentrale Elemente wie Resilienzpläne, Wiederanlaufstrategien, Lieferkettenkontrollen oder Rollenmodelle für Krisenlagen sind künftig nicht nur organisatorisch sinnvoll, sondern gesetzlich gefordert. Damit verbunden ist die Notwendigkeit, verschiedene internationale Normen, insbesondere ISO 31000 (Risikomanagement), ISO 22301 (Business Continuity) und ISO 27001 (Informationssicherheit) sowie je nach Kontext auch ISO 28000 (Sicherheitsmanagement in Lieferketten) und ISO 30401 (Wissensmanagement), in bestehende Managementsysteme zu integrieren.

Resilienz wird normativ: Was jetzt auf Stadtwerke zukommt

- CER-Richtlinie (EU): verlangt sektorspezifische Resilienzmaßnahmen und Notfallpläne (Art. 12/13)
- NIS2 und KRITIS-Dachgesetz (in Vorbereitung): dehnen Sicherheits- und Resilienzpflichten auch auf Betreiber unterhalb klassischer KRITIS-Schwellen aus

Relevante Normen im Überblick:

Norm	Funktion
ISO 31000	Risikomanagement als Steuerungsrahmen
ISO 27001	Schutz informationsverarbeitender Systeme
ISO 22301	Wiederanlaufplanung und Krisenorganisation
ISO 28000	Lieferkettensicherheit und Partnerrisiken
ISO 30401	Wissenserhalt und Lessons Learned Management

Diese Normen greifen ineinander. Es fehlt jedoch an praxisnahen Umsetzungshilfen, insbesondere für kommunale Versorger mit dezentraler Struktur.

Empfehlung: Frühzeitige Orientierung an ISO 31000 und gezielter Ausbau modularer Prozesse, ergänzt durch sektorale Umsetzungshilfen, Pilotprojekte oder Branchenstandards (z. B. durch BDEW, BNetzA und BSI).

Gerade für kleinere und mittelgroße Stadtwerke stellt diese Entwicklung eine erhebliche Herausforderung dar. Es fehlen bislang abgestimmte Umsetzungshilfen, wie sich diese Normen in übergreifende Managementstrukturen einbinden lassen, insbesondere unter dem Primat knapper Ressourcen und dezentraler Verantwortlichkeiten. Der Einstieg in ein strukturiertes Risikomanagement nach ISO 31000 kann hier eine erste Orientierung bieten. Darüber hinaus ist jedoch eine praxisgerechte, modulare Operationalisierung erforderlich, die auch nicht zertifizierungspflichtige Häuser adressiert.

Die künftige Resilienzfähigkeit kommunaler Energieversorgung wird wesentlich davon abhängen, wie gut es gelingt, Regelanforderungen mit betrieblicher Realität zu verzahnen. Dafür braucht es sektorspezifische Hilfestellungen, integrierte Werkzeuge und Umsetzungsleitfäden, die technische, organisatorische und strategische Resilienzanforderungen konsolidiert abbilden und es damit auch kleineren Versorgern ermöglichen, ihre Systeme zukunftssicher aufzustellen.

3.3 Fazit und Handlungsperspektiven

Die vorangegangenen Kapitel haben gezeigt, dass integrierte Stadtwerke in einem vielschichtigen Spannungsfeld agieren: zwischen historisch gewachsenen OT-Systemen und modernen IT-Infrastrukturen,

zwischen funktional verteilten Zuständigkeiten und überlagernden Marktrollen sowie zwischen immer komplexer werdenden regulatorischen Anforderungen auf nationaler und europäischer Ebene.

Die Fallstudie ist als realitätsnah, aber lediglich als Blaupause zu verstehen. In einer konkreten Instanz würde sie voraussichtlich weiteren Bedarf an Harmonisierungen auf tieferer Ebene offenlegen, etwa im Kontext des Mappings von Schutzkatalogen oder der Priorisierung und Budgetierung. Insbesondere im Rahmen eines strukturierten Risikomanagementprozesses nach dem international anerkannten Standard ISO 31000 treten solche Aspekte deutlich hervor.

Weitere Arbeiten innerhalb der Branchenplattform könnten dazu beitragen, an diesen Schnittstellen gezielt Mehrwerte und Umsetzungshilfen zu entwickeln. Klassische ISMS adressieren viele dieser Anforderungen formal, bleiben jedoch häufig innerhalb definierter Systemgrenzen. Sie sind in der Regel auf einzelne Organisationseinheiten, Assets oder Prozesslandschaften zugeschnitten und stoßen dort an Grenzen, wo Sicherheitsverantwortung über mehrere Marktrollen, Technikgenerationen und externe Dienstleister hinweg verteilt ist (vgl. Tabelle 7).

	Klassisches ISMS (z. B. ISO 27001)	Anforderungen im integrierten Stadtwerk
Systemgrenzen	Fokussiert auf definierte Assets, IT-Infrastruktur oder Organisationseinheiten	Überschreitende Zuständigkeiten zwischen Netzbetrieb, GWA, Marktkommunikation und OT-Systemen
Auditlogik	Standardisierte Auditpfade, meist IT-orientiert	Heterogene Prüfregime (ISO, TR, B3S, Herstellerstandards), keine durchgehende Prüfstruktur
Rollenverständnis	Klare Rollenzuweisung innerhalb homogener ISMS-Strukturen	Überlagerung von Marktrollen (z. B. Netzbetreiber, gMSB und GWA) in einer Organisationseinheit
Lieferantenintegration	Lieferanten oft als „Dritte“ mit klarer Schnittstelle	Tief eingebettete Dienstleister (z. B. CLS-Dienste, Hosting, Fernwartung), schwierige Governance
Risikobetrachtung	Fokus auf Informationssicherheit und Datenschutz	Kombination aus Informations-, OT-, Prozess- und Versorgungssicherheit
Governance	Sicherheitsmanagement als Fachfunktion	Erfordert Anbindung an Geschäftsführung, Technik, Betrieb und kommunale Aufsicht
Zertifizierbarkeit	Formal gut prüfbar durch normierte Anforderungen	Hohe Umsetzungs- und Nachweiskomplexität bei hybrider Systemlandschaft

Tabelle 7: Grenzen klassischer ISMS-Modelle im integrierten Stadtwerk

Auch die eingesetzten Audit- und Zertifizierungsverfahren weisen methodische Lücken auf: Sie prüfen isolierte Teilbereiche, ohne ihre Interdependenzen systematisch zu bewerten. Für integrierte Stadtwerke entsteht eine besondere Herausforderung:

Die technischen Realitäten erfordern eine ganzheitliche Sicherheits- und Resilienzbetrachtung, die klassische ISMS-Ansätze nicht ohne Weiteres leisten können.

Stattdessen bedarf es eines erweiterten Steuerungsmodells, das Governance sowie Risiko- und Notfallmanagement mit hybrider Systemarchitektur, Marktanforderungen und begrenzten Ressourcen in Einklang bringt.

Das integrierte Stadtwerk braucht daher einen ganzheitlicheren Blick auf Resilienz – einen Blick, der technische, organisatorische und strategische Ebenen systematisch miteinander verknüpft. Das folgende Kapitel strukturiert die gewonnenen Erkenntnisse und leitet daraus konkrete Handlungsfelder ab, die den Einstieg in eine integrierte Resilienzsteuerung unterstützen können.

3.3.1 Systemische Herausforderungen im Überblick

Die Analyse des fiktiven integrierten Stadtwerks hat zentrale systemische Herausforderungen offengelegt, die nicht nur punktuell auftreten, sondern strukturell im Aufbau kommunaler Versorgungsorganisationen verankert sind. Sie lassen sich in fünf übergreifende Problembereiche gliedern:

1) Hybride Systemlandschaften: Die Koexistenz unterschiedlicher Systemgenerationen erschwert die konsistente Umsetzung von Sicherheitsstrategien. Unterschiede in Lebenszyklen, Patch-Fähigkeit und Kommunikationsprotokollen führen zu Modernisierungsasymmetrien und technischen Bruchstellen.

2) Fragmentierte Zuständigkeiten und Rollenüberschneidungen: Die funktionale Integration von Netzbetrieb, Messwesen, Marktkommunikation und IT-Betrieb innerhalb einer Organisationseinheit erzeugt komplexe Verantwortungsstrukturen. Ohne klare Zuständigkeiten und durchgängige Steuerungsmodelle entstehen Schnittstellenrisiken, etwa bei Störungen oder bei der Umsetzung regulatorischer Vorgaben.

3) Divergierende Prüf- und Zertifizierungsregime: Unterschiedliche Anforderungen aus ISO 27001, BSI-Richtlinien, Branchenspezifischen Sicherheitsstandards und regulatorischen Vorgaben der BNetzA treffen im integrierten Stadtwerk aufeinander.

4) Abhängigkeiten von Dritten: Der zunehmende Einsatz spezialisierter externer Dienstleister und Hersteller bringt Transparenzdefizite, Steuerungslücken und Lock-in-Effekte mit sich. Gleichzeitig bleiben viele dieser Partner außerhalb des unmittelbaren Governance-Rahmens.

5) Strategisch-regulatorische Unschärfe: Viele Sicherheitsvorgaben bewegen sich auf einem hohen Abstraktionsniveau und sind bislang nur unvollständig in nationales Recht überführt. Für kommunale Akteure ergibt sich daraus erheblicher Interpretationsbedarf, verbunden mit Unsicherheit hinsichtlich künftiger Prüfmaßstäbe und Umsetzungspflichten.

Diese Herausforderungen greifen ineinander und entfalten ihre Wirkung entlang der gesamten System- und Prozesskette. Um ihnen wirkungsvoll begegnen zu können, bedarf es eines integrierten Ansatzes, der technische, organisatorische und strategische Steuerungselemente zusammenführt.

Adressierte Akteure: Die hier beschriebenen Herausforderungen betreffen insbesondere integrierte Stadtwerke als unmittelbar betroffene Akteure. Für die gezielte Unterstützung bei der Systematisierung, Standardisierung und methodischen Aufbereitung sind zudem Branchenverbände und die Branchenplattform gefordert. Politik und Regulierung sollten flankierend tätig werden, um durch Klarstellungen in Rechtsnormen und Aufsichtspraxis Planbarkeit zu schaffen.

3.3.2 Handlungsperspektiven auf operativer Ebene

Trotz begrenzter Ressourcen und komplexer Rahmenbedingungen verfügen integrierte Stadtwerke über konkrete Ansatzpunkte, um ihre Sicherheits- und Resilienzarchitektur schrittweise zu stärken. Im Fokus

stehen dabei praktikable Maßnahmen, die an bestehende Strukturen anknüpfen und zugleich systemische Schwachstellen adressieren:

Integrierte Stadtwerke operieren vielfach unter schwierigen Rahmenbedingungen: knappe Ressourcen, hochgradig vernetzte Prozesse und fragmentierte Zuständigkeiten. Dennoch lassen sich durch gezielte Maßnahmen erhebliche Fortschritte erzielen.

Diese Maßnahmen lassen sich modular in bestehende Strukturen integrieren und bilden die Grundlage für ein resilienteres, übergreifendes Sicherheitsmanagement, auch unterhalb formaler KRITIS-Schwellen. Ausgewählte, sehr wirkungsvolle Maßnahmen sind:

- **Schnittstellenmanagement stärken:** Einführung verbindlicher Dokumentations- und Zuständigkeitsmodelle an OT-/IT-Übergabepunkten; Definition von technischen und organisatorischen Interface-Kontrollen
- **Segmentierung konsequent umsetzen:** Technisch-logische Trennung von IT- und OT-Netzen inklusive dedizierter Gateway-Zonen und Kommunikationsfilter
- **Lifecycle-Management ausbauen:** Einführung eines ganzheitlichen Patch-, Update- und Ersatzteilkonzepts unter Einbindung externer Systemanbieter
- **Dienstleistersteuerung professionalisieren:** Einführung standardisierter Sicherheitsvereinbarungen (z. B. Security Annex in Service Level Agreements), Auditpflichten und Monitoring-Strukturen
- **Vorfallmanagement integrieren:** Entwicklung eines einheitlichen, systemübergreifenden Incident-Response-Modells mit Rollenklärung, Eskalationswegen und technischer Alarmierung

Adressierte Akteure: Die beschriebenen operativen Maßnahmen richten sich vorrangig an integrierte Stadtwerke und vergleichbare kommunale Versorger. Die Branchenplattform sollte unterstützend wirken, indem sie praxiserprobte Musterlösungen, Checklisten und Umsetzungshilfen bereitstellt. Branchenverbände sind gefordert, diese Erfahrungen zu bündeln und in sektorspezifische Mindestanforderungen zu überführen.

3.3.3 Handlungsperspektiven auf strategischer Ebene

Die strukturelle Komplexität integrierter Stadtwerke erfordert nicht nur technische und prozessuale Anpassungen, sondern auch eine strategische Neuausrichtung der Sicherheits-Governance. Viele Herausforderungen lassen sich nur durch eine verankerte, ressortübergreifende Steuerung adressieren.

Die Stärkung der Resilienzfähigkeit erfordert strukturelle Anpassungen in der Governance und strategischen Steuerung.

- **Governance-Strukturen aufbauen:** Einrichtung von zentralen Sicherheits- und Resilienzgremien mit Beteiligung aller betroffenen Funktionsbereiche (Netzbetrieb, IT, GWA, Vertrieb)
- **Verantwortlichkeiten schärfen:** Rollendefinitionen entlang der Prozesskette systematisch abbilden und in Steuerungsinstrumente (Risikomanagement, Auditpläne, Eskalationsketten) überführen
- **Sicherheitskultur verankern:** Aufbau strukturierter Awareness-Programme inklusive Schulung, Reporting-Mechanismen und Lernschleifen nach Störungen
- **Kommunale Steuerung einbinden:** Aufsichtsgremien und Gesellschafter frühzeitig in Sicherheitsfragen einbeziehen und mit strategischen Entscheidungsgrundlagen versorgen

Die strategische Weiterentwicklung der Sicherheitssteuerung stößt in vielen Fällen an systemische Grenzen, etwa bei der Frage, wie Resilienz in interorganisationalen Funktionsketten nachweisbar und steuerbar wird. Daraus ergeben sich klare Anforderungen an zukünftige Forschungs- und Entwicklungsvorhaben.

Adressierte Akteure: Die strategische Neuausrichtung der Sicherheits-Governance betrifft vor allem die kommunalen Träger und Aufsichtsgremien, die entsprechende Steuerungsstrukturen verankern müssen. Die Branchenplattform kann hier durch Governance-Modelle und Argumentationshilfen unterstützen. Gleichzeitig sind politische Entscheidungsträger und Regulierungsbehörden gefordert, bestehende Zielkonflikte, etwa zwischen Risikoorientierung und Nachweispflichten, aufzulösen.

3.3.4 Weiterführende Untersuchungs- und Entwicklungsbedarfe

Integrierte Stadtwerke benötigen neue Steuerungsmodelle, um mit hybriden Systemstrukturen, regulatorischer Unschärfe und funktionaler Abhängigkeit wirksam umzugehen. Die bisherigen Sicherheits- und ISMS-Modelle bieten hierfür wichtige Grundlagen, genügen aber nicht mehr den Anforderungen einer prozess- und funktionsbezogenen Resilienzsteuerung. Daraus ergeben sich konkrete Entwicklungsbedarfe für die Branche, organisiert etwa in den Fachgruppen der Verbände oder Branchenplattformen.

1) Entwicklung eines integrierten Resilienzkonzepts für kommunale Energieversorger

Es fehlt bislang ein methodisch fundiertes und praxisnahes Referenzmodell, das Sicherheits-, Notfall- und Risikomanagement zu einem ganzheitlichen Resilienzansatz zusammenführt. Dieses Konzept sollte folgende Komponenten berücksichtigen:

- Integration technischer Sicherheit (IT/OT) mit organisatorischer Resilienz (z. B. Rollenmodell, Vertretungskonzepte, Störfallmanagement)
- Verknüpfung mit Governance-Strukturen, Budgetsteuerung und Investitionsprozessen
- Einbettung externer Dienstleister und Lieferanten in das Resilienzverständnis
- Ausrichtung auf verschiedene Bedrohungsszenarien: Cyberangriffe, Systemausfälle, regulatorische Friktionen, Lieferkettenstörungen

Weiterhin können sich Sicherheits- und Resilienzstrategien im Energiesektor nicht länger auf einzelne Organisationen, Technologien oder Rollen beschränken. In der heutigen Versorgungsrealität entsteht Resilienz nicht innerhalb isolierter Zuständigkeiten, sondern im Zusammenspiel kritischer Funktionen, Prozesse und Systeme sowie über organisatorische und technische Grenzen hinweg. Zukünftige Resilienzkonzepte sollten daher nicht primär technologie- oder betriebsbezogen, sondern funktionsorientiert gestaltet werden.

2) Künftige Studien zur Umsetzbarkeit von Sicherheitsvorgaben in KMU-Strukturen

Es besteht aus Sicht der Autoren erheblicher Bedarf, die Übersetzbarkeit strategischer Sicherheitsvorgaben (z. B. NIS2, CER, AI Act) in operative Realität kleiner und mittlerer Versorgungsunternehmen durch die Branchenplattform zu bewerten und Handlungsempfehlungen auszuarbeiten. Zentrale Aufgabenstellungen lauten:

- Welche Umsetzungspfade sind realistisch bei begrenzten personellen und finanziellen Ressourcen?
- Wie lassen sich europäische Anforderungen mit nationaler Gesetzgebung (z. B. KRITIS-DachG, BSIG) systematisch abgleichen?
- Welche Formen von Unterstützung (z. B. Branchenleitfäden, Toolkits, Trainingsformate) sind wirksam?

Zentral für einen funktionsorientierten Resilienzansatz ist die gezielte Betrachtung dessen, was tatsächlich für die Versorgungssicherheit und den Systembetrieb entscheidend ist, unabhängig davon, ob diese Elemente in einer Organisation oder verteilt über mehrere Akteure liegen. Dabei lassen sich Kategorien unterscheiden: Zum einen sind dies kritische Funktionen, also essenzielle Aufgaben wie die Redispatch-Steuerung, die Netzführung, die Leistungs- und Frequenzregelung oder der Betrieb des CLS-Kommunikationskanals. Diese Funktionen sind unmittelbar mit dem Betrieb der Infrastruktur verknüpft und müssen auch unter Stör- oder Krisenbedingungen verfügbar bleiben. Zum zweiten geht es um kritische Prozesse, die nicht isoliert in einem System stattfinden, sondern das koordinierte Zusammenwirken mehrerer Akteure, Systeme und Datenflüsse erfordern. Beispiele hierfür sind Eskalationen im Kontext des § 14a EnWG, Redispatch-Interaktionen zwischen Übertragungsnetzbetreibern und grundzuständigen Messstellenbetreibern oder auch durchgängige Kommunikationsketten zwischen AS4-Servern, Formatprüfern, ERP-Systemen und externen Plattformen. Schließlich zählen auch kritische Systeme dazu, deren technisches Zusammenspiel besonders engmaschig und störanfällig ist. Hierzu gehören etwa SCADA-Leitsysteme, Gateway-Administrations-Backends (GWA), Bilanzierungsplattformen oder moderne MDMS, die meist in komplexen technischen Ketten integriert sind und deren Störung weitreichende Auswirkungen haben kann.

Solche Funktionen lassen sich nicht allein durch ein vereinzeltes Unternehmen absichern. Ihre Resilienz ergibt sich erst durch abgestimmte Prozesse zwischen Stadtwerken, Netzbetreibern, Anlagenbetreibern, IT-Providern und Plattformbetreibern entlang gemeinsamer Schnittstellen, Reaktionsmuster und Rollenmodelle.

3) Resilienzarchitekturen im Marktverbund

Ein zukunftsfähiger Resilienzansatz im Energiesektor muss über die Grenzen einzelner Organisationen hinausdenken. Die zunehmende funktionale Vernetzung technischer Systeme und betrieblicher Rollen erfordert neue Forschungsimpulse, um Resilienz nicht nur innerhalb eines Stadtwerks oder eines Netzbetreibers zu sichern, sondern auch im kooperativen Marktverbund.

Kritische Funktionen wie Redispatch, Netzführung, CLS-Betrieb oder Marktkommunikation sind heute interorganisatorisch verzahnt. Ihre Resilienz kann nicht mehr allein auf Ebene eines einzelnen Betreibers gewährleistet werden. Klassische ISMS stoßen hier an Grenzen, da sie auf klar abgegrenzte Organisationseinheiten fokussieren.

Erforderlich sind neue Resilienzmodelle, die

- funktionsübergreifend entlang gemeinsamer Kernprozesse wirken,
- technische Interdependenzen und verteilte Zuständigkeiten abbilden,
- Wiederanlauf-, Incident- und Lieferkettenprozesse koordiniert steuern und
- auch vertragliche, regulatorische und organisatorische Schnittstellen systematisch einbeziehen.

Resilienz-Fragestellungen gewinnen insbesondere im Lichte aktueller europäischer Regulierungen wie NIS2 und CER-Verordnung oder des KRITIS-Dachgesetzes an Bedeutung. Sie setzen auf eine funktionale Betrachtung von Versorgungssicherheit und fordern explizit die Einbindung Dritter sowie sektorübergreifende Koordination. Für mittelständische, kommunale und kooperative Marktstrukturen liegen bislang jedoch weder methodisch belastbare Umsetzungskonzepte noch praxistaugliche Referenzmodelle vor.

Adressierte Akteure: Die in diesem Abschnitt beschriebenen Entwicklungsbedarfe betreffen mehrere Akteursebenen:

- Branchenplattformen (z. B. dena) sollten die methodische Entwicklung funktionsbasierter Referenzmodelle, Mappings zwischen Schutzkatalogen und sektorübergreifender Schnittstellenmodelle koordinieren und in Pilotprojekten erproben.
- Branchenverbände sind gefordert, den Austausch über Best Practices zu verstetigen, spezifische Anforderungen kommunaler Versorger zu bündeln und sie in politische Debatten einzuspeisen. Sie spielen zudem eine Schlüsselrolle bei der Priorisierung und der Unterstützung des Transfers in die Fläche.
- Politik und Regulierung (insbesondere BMWE, BSI und BNetzA) sollten bestehende Unschärfen in der Auslegung europäischer Vorgaben (NIS2, CER, KRITIS-DachG) konkretisieren, funktionale Schwellenwerte definieren und klare Zuständigkeitsmodelle für verteilte Betreiberverantwortung etablieren. Dies ist vor allem relevant für Akteure, die KRITIS-nahe Funktionen übernehmen, aber formal nicht als KRITIS-Betreiber gelten.
- Schließlich sind auch IT-Dienstleister, Plattformbetreiber und systemnahe Drittanbieter angesprochen, die ihre Lösungen an gemeinsamen Referenzarchitekturen ausrichten und sich aktiv in eine koordinierte Resilienzsteuerung einbringen sollten.

4 Anhang

Anhang A: Zentrale Gesetze, Normen, Richtlinien und Standards

Zur besseren Einordnung der in Kapitel 2 beschriebenen Sicherheitsanforderungen und Prüfverfahren bietet die folgende Übersicht eine Zusammenstellung der zentralen Normen, Richtlinien und regulatorischen Grundlagen.

	Regelwerk	Ziel	Anwendungskontext
Gesetzliche Grundlagen	§ 8a und 9b BSIG (BSIG, 2023)	Vorgaben zur Absicherung und Zulassung kritischer Komponenten und Systeme	KRITIS-Betreiber, Hersteller sicherheitsrelevanter Komponenten, BSI als Zulassungs- und Prüfbehörde
	§ 11 Abs. 1a und 1b EnWG (EnWG, 2023)	Verpflichtung zum Betrieb eines Informationssicherheitsmanagementsystems (ISMS) für Netz- und Energieanlagenbetreiber	Energieversorger und Netzbetreiber; Basis für ISMS-Zertifizierung gemäß BNetzA-IT-Sicherheitskatalog
	Messstellenbetriebsgesetz (MsbG, 2023)	Rechtlicher Rahmen für das intelligente Messwesen	gMSB, wMSB und GWA: Anforderungen an Betrieb, Sicherheit und Zertifizierung intelligenter Messsysteme
	NIS2-Richtlinie, Artikel 21, 23 (EU, 2022)	Einheitliche Cybersicherheitsvorgaben in der EU: Risiko- und Sicherheitsmanagement, Vorfallmeldung	Betreiber wesentlicher und wichtiger Einrichtungen, IKT-Dienstleister, Softwareanbieter; verpflichtet zur ISMS-Einführung und Vorfallmeldung
	Cyber Resilience Act (Entwurf) (EU, 2024)	Sicherheitsanforderungen und Zertifizierungspflicht für digitale Produkte	Hersteller sicherheitskritischer Software und Hardwarekomponenten in der EU
Sicherheitskataloge	IT-Sicherheitskatalog Energieanlagen (BNetzA) (BNetzA, 2015)	ISMS-Pflicht für Betreiber von Energieanlagen nach § 11 EnWG	Energieanlagenbetreiber (z. B. Kraftwerksbetreiber); Grundlage für Zertifizierung nach International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC) 27001 + Zusatzforderungen
	Konformitätsbewertungsprogramm Energieanlagen (BNetzA, 2022a)	Bewertungsverfahren für ISMS-Zertifizierungen nach dem Sicherheitskatalog Energieanlagen	Auditierer, Zertifizierungsstellen, BNetzA; Grundlage für akkreditierte ISMS-Prüfungen gemäß § 11 EnWG
	IT-Sicherheitskatalog Energienetze	ISMS-Pflicht für Netzbetreiber nach § 11 EnWG	Übertragungs- und Verteilnetzbetreiber; Grundlage für Zertifizierung nach ISO/IEC 27001 + Zusatzforderungen
	Konformitätsbewertungsprogramm Energienetze	Bewertungsverfahren für ISMS-Zertifizierungen nach dem Sicherheitskatalog Energienetze	Auditierer, Zertifizierungsstellen, BNetzA; Grundlage für akkreditierte ISMS-Prüfungen gemäß § 11 EnWG
	Branchenspezifischer Sicherheitsstandard (B3S)	BSI-anerkannter ISMS-Standard für Stromaggregatoren zur Erfüllung der Anforderungen gemäß § 8a BSIG	Betreiber virtueller Kraftwerke, Flexibilitätsvermarkter, Redispatch-Plattformen bei Überschreitung KRITIS-relevanter Schwellenwerte

Sicherheits-kataloge	für Aggrega-toren		
	Bundesverband der Energie- und Wasserwirt-schaft (BDEW) – Whitepaper Informations-sicherheit	Branchenempfehlung für ISMS-Implementierung in der Energie-wirtschaft	Energieversorger, Netzbetreiber, IT-Dienstleister; oft Basis für Entwick-lung von B3S und internen Richt-linien
Informations-sicherheits-management-systeme	ISO/IEC 27001	Internationaler Standard für Auf-bau, Betrieb und Zertifizierung eines ISMS	Grundlage für ISMS-Zertifizierungen gemäß § 11 EnWG, § 8a BSIG sowie B3S; anwendbar in regulierten und nicht regulierten Sektoren
	ISO/IEC 27002	Leitfaden mit Maßnahmenempfeh-lungen zur Umsetzung von ISO/IEC 27001	IT- und OT-Sicherheitsverantwort-liche, CISO, Auditierer; dient zur Strukturierung und Auswahl geeig-neter Sicherheitsmaßnahmen
	ISO/IEC 27019	Branchenspezifische Erweiterung der ISO/IEC 27002 für OT in der Energieversorgung	Verbindlich bei ISMS-Zertifizie-rungen im Energiesektor; relevant für Netz- und Anlagenbetreiber, Aggregatoren, Smart-Grid-Platt-formen
	BSI-IT-Grundschutz-Kompendium	Modulares Regelwerk zur systema-tischen Absicherung von IT-Syste-men nach BSI-Vorgaben	Grundlage freiwilliger ISMS-Zertifi-zierungen oder Nachweisführung gemäß § 8a BSIG, insbesondere bei Behörden und ISO-fremden Struk-turen
Technische Vorgaben / Produktanfor-derungen	TR-03109	BSI-Richtlinie für Smart Meter Gateways und ihre Backend-Systeme	GWA, Smart-Meter-Hersteller, Backend-Betreiber; Voraussetzung für BSI-Zertifizierung gemäß § 24 MsbG
	TR-02102	Anforderungen an den Einsatz sicherer kryptografischer Verfahren	Alle sicherheitskritischen Systeme mit Verschlüsselungspflicht; gilt als „Stand der Technik“
	TR-03116	Anforderungen an sichere Netzkom-munikation (z. B. Virtual Private Network (VPN), TLS, Zertifikats-nutzung)	Betreiber von Leittechnik-, Fern-wirk- und Messinfrastrukturen; u. a. in Smart Grids und Automatisie-rungssystemen
	TR-03122 / TR-03130 / TR-03124	Technische Richtlinien zu Identitäts-management und Authentifizierung	Relevanz für Marktkommunikation, Public-Key-Infrastrukturen (PKI), eID-Systeme, Smart Meter PKI
	Common Criteria (CC) / ISO/IEC 15408	Internationales Evaluierungs-schema für sicherheitsrelevante IT-Produkte	Grundlage für die Entwicklung und Bewertung von Schutzprofilen und BSI-Zertifizierungen; u. a. für Smart Meter Gateways
	BSI-CC-PP-0073	Schutzprofil für Smart Meter Gate-ways zur Erfüllung der TR-03109-Anforderungen	Hersteller von zertifizierungspflich-tigen Smart Meter Gateways; muss vollständig erfüllt sein für BSI-Zulas-sung

Tabelle 8: Zentrale Gesetze, Normen, Richtlinien und Standards im Kontext energiewirtschaftlicher Cybersicherheit

Anhang B: Übersicht über die Handlungsempfehlungen aus Kapitel 2 und 3

	Handlungsfeld	Adressierte Akteure	Nutzen/Ziel
Kapitel 2	Modulare Prüfverfahren und gegenseitige Anerkennung	Politik, Aufsichtsbehörden	Doppelprüfungen vermeiden, Effizienz steigern, Betreiber entlasten
	Hybride Prüfmodelle und dialogische Aufsicht	Aufsichtsbehörden	Prüfbarkeit erhöhen, Vertrauen stärken
	Wiederverwendung von Nachweisen	Branchenplattform, Verbände	Redundanzen reduzieren, Prüfkosten senken
	Qualifikationsstandards für Prüfer	Politik, Akkreditierungsstellen	Vergleichbare Prüfqualität sicherstellen
	Zertifikatsregister und Audit-plattformen	EU-Politik, Branchenverbände	Transparenz erhöhen, Nachweislast reduzieren
Kapitel 3	Systemische Herausforderungen adressieren	Stadtwerke, Branchenplattform, Politik	Risiken durch Strukturdefizite reduzieren
	Operative Resilienzmaßnahmen	Stadtwerke, Branchenplattform, Verbände	Pragmatische Umsetzung auch unterhalb KRITIS-Schwelle ermöglichen
	Strategische Sicherheits-Governance	Kommunale Träger, Branchenplattform, Politik	Verantwortung verankern, ressortübergreifende Steuerung stärken
	Entwicklung funktionsbasierter Resilienzmodelle	Branchenplattform, Verbände, Politik, Technikakteure	Resilienz in verteilten Systemen steuerbar machen
	Integriertes Resilienzkonzept für kommunale Energieversorger	Branchenplattformen, kommunale Unternehmen, Politik	Systemisch abgestimmte Resilienzstrategien über technische und organisatorische Ebenen hinweg
	Studien und Tools zur Umsetzung regulatorischer Vorgaben in KMU	Aufsichtsbehörden, Forschungsakteure, Verbände	Praxisgerechte Unterstützung für kleine und mittlere Versorger bei NIS2, CER, KRITIS-Dachgesetz etc.

Abbildungsverzeichnis

Tabellenverzeichnis

Literaturverzeichnis

Bundesamt für Sicherheit in der Informationstechnik (BSI, 2018): Technische Richtlinie BSI TR-03116-1, Kryptographische Vorgaben für Projekte der Bundesregierung. Teil 1: Telematikinfrastruktur. Version 3.20. Bonn.

Bundesamt für Sicherheit in der Informationstechnik (BSI-1, 2019): Protection Profile BSI-CC-PP-0073, Smart Meter Gateway. Version 1.4, Stand: 19. März 2019.

Bundesamt für Sicherheit in der Informationstechnik (BSI-2, 2019): Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz, Zertifizierungsschema. Version 2.1. Bonn.

Bundesamt für Sicherheit in der Informationstechnik (BSI-1, 2020): Technische Richtlinie BSI TR-03130, eID-Server, Teil 1: Technische Anforderungen. Version 1.14, Stand: Februar 2020. Bonn.

Bundesamt für Sicherheit in der Informationstechnik (BSI-2, 2020): Technische Richtlinie BSI TR-03124, eID-Client, Teil 1: Grundlagen und Architektur. Version 1.5, Stand: März 2020. Bonn.

Bundesamt für Sicherheit in der Informationstechnik (BSI, 2021): BSI-Standard 200-1, Managementsysteme für Informationssicherheit (ISMS). Version 1.1, Stand: Oktober 2021. Bonn.

Bundesamt für Sicherheit in der Informationstechnik (BSI-1, 2022): Common Criteria (CC), IT-Sicherheitskriterien gemäß ISO/IEC 15408:2022 und Evaluationsmethodologie ISO/IEC 18045:2022.

Bundesamt für Sicherheit in der Informationstechnik (BSI-2, 2022): Technical Guideline BSI TR-03122-1, eCard-API-Framework, Part 1: Overview. Version 6.0. Bonn.

Bundesamt für Sicherheit in der Informationstechnik (BSI, 2023): IT-Grundschutz-Kompendium, Edition 2023. Systematischer Einstieg in das Management der Informationssicherheit. Stand: Februar 2023. Bonn.

Bundesamt für Sicherheit in der Informationstechnik (BSI-1, 2024): BSI TR-03109, Dachdokument Technische Richtlinie BSI TR-03109 für intelligente Messsysteme. Version 2.2. Bonn.

Bundesamt für Sicherheit in der Informationstechnik (BSI-2, 2024): Verfahrensbeschreibung zur Zertifizierung von Produkten, Prozessen und Dienstleistungen. Version 5.1 vom 31. Juli 2024. Bonn.

Bundesamt für Sicherheit in der Informationstechnik (BSI-1, 2025): Anforderungen nach § 8a Absatz 5 BSIG, Grundsätzliche Anforderungen im Nachweisverfahren (GAiN). Version 2.1. Bonn.

Bundesamt für Sicherheit in der Informationstechnik (BSI-2, 2025): Technische Richtlinie TR-02102-2, Kryptographische Verfahren: Empfehlungen und Schlüssellängen. Version 2025-01. Bonn.

Bundesnetzagentur (BNetzA, 2015): IT-Sicherheitskatalog gemäß § 11 Absatz 1a Energiewirtschaftsgesetz. Stand: August 2015. Bonn.

Bundesnetzagentur (BNetzA, 2022a): Konformitätsbewertungsprogramm für Energieanlagen nach § 11 Abs. 1b EnWG. Stand: 24. März 2022. Bonn.

Bundesnetzagentur (BNetzA, 2022b): IT-Sicherheitskatalog für Betreiber von Energieanlagen nach § 11 Abs. 1b EnWG. Stand: 24. März 2022. Bonn.

Bundesnetzagentur (BNetzA, 2022c): Festlegung BK6-22-300: Festlegung zur IT-Sicherheit nach § 11 Abs. 1b EnWG für Betreiber von Energieanlagen. Stand: 24. März 2022. Bonn.

Bundesnetzagentur (BNetzA, 2025): Konsultationsfassung der Eckpunkte zur Festlegung – Erstellung eines IT-Sicherheitskatalogs nach § 11 Abs. 1a und 1b EnWG, Zeilen 146-148, Stand: 07. Mai 2025. Bonn.

Bundesnetzagentur (BNetzA, o. D.): Verbindliche Erklärung des Netzbetreibers zur Nichtanwendbarkeit des IT-Sicherheitskatalogs für Strom- und Gasnetze gemäß § 11 Absatz 1a Energiewirtschaftsgesetz (EnWG). Bonn.

Bundesrepublik Deutschland (BSIG, 2023): BSIG, Zertifizierung von Sicherheit in der Informationstechnik. In: Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG). Stand: 14. August 2009, zuletzt geändert am 20. November 2023.

Bundesrepublik Deutschland (EnWG, 2023): § 11 Abs. 1a–1b EnWG, Anforderungen an Telekommunikations- und IT-Systeme in Energieversorgungsnetzen. In: Gesetz über die Elektrizitäts- und Gasversorgung (Energiewirtschaftsgesetz, EnWG). Stand: 7. Juli 2005, zuletzt geändert am 20. November 2023.

Bundesrepublik Deutschland (MsbG, 2023): Gesetz über den Messstellenbetrieb und die Datenkommunikation in intelligenten Energienetzen (Messstellenbetriebsgesetz, MsbG). Stand: 29. August 2016, zuletzt geändert am 20. November 2023.

Bundesrepublik Deutschland (BSI-KritisV, 2023): Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung, BSI-KritisV). Stand: 22. April 2016, zuletzt geändert am 20. November 2023. Bonn.

Bundesverband der Energie- und Wasserwirtschaft (BDEW, 2023): Branchenspezifischer Sicherheitsstandard (B3S) für Anlagen oder Systeme zur Steuerung / Bündelung elektrischer Leistung, Version 1.2. Anerkannt durch das BSI nach § 8a BSIG. Stand: 13. Januar 2023. Berlin.

Bundesverband der Energie- und Wasserwirtschaft (BDEW, 2024): Anforderungen an sichere Steuerungs- und Telekommunikationssysteme. Aarau, Berlin, Wien.

Europäische Union (EU, 2022): Art. 21 & Art. 23 der Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union (NIS-2-Richtlinie).

Europäische Union (EU, 2024): Verordnung (EU) 2024/858 des Europäischen Parlaments und des Rates vom 13. März 2024 über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen und zur Änderung der Verordnung (EU) 2019/1020, Cyber-Resilience-Act (CRA).

European Telecommunications Standards Institute (ETSI, 2020): ETSI EN 303 645 V2.1.1 (2020-06), Cyber Security for Consumer Internet of Things: Baseline Requirements. Sophia Antipolis, Frankreich.

European Union Agency for Cybersecurity (ENISA, 2012): Smart Grid Security, Recommendations for Europe and Member States. Stand: 1. Juli 2012. Heraklion, Griechenland.

European Union Agency for Cybersecurity (ENISA, 2024): Cyber Resilience Act Requirements Standards Mapping. Online verfügbar unter: https://www.enisa.europa.eu/publications/cyber-resilience-act-requirements-standards-mapping [zuletzt abgerufen am 24. Juni 2025].

Abkürzungen

API	Application Programming Interface
AS4	Applicability Statement 4
B2B	Business to Business
B3S	Branchenspezifischer Sicherheitsstandard
BDEW	Bundesverband der Energie- und Wasserwirtschaft
BMWE	Bundesministerium für Wirtschaft und Energie
BNetzA	Bundesnetzagentur
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSIG	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik
BSI-IT	BSI-IT-Grundschutz
BSI-KritisV	Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz
BSI-TR	Technische Richtlinie des BSI
CC	Common Criteria
CER	Critical Entities Resilience Directive
CLS	Controllable Local System
CRA	Cyber Resilience Act
CRM	Customer Relationship Management
DAkkS	Deutsche Akkreditierungsstelle
DIN	Deutsches Institut für Normung
DPI	Deep Packet Inspection
DQR	Deutscher Qualifikationsrahmen
EEX	European Energy Exchange
eID	Elektronische Identität
EN	Europäische Norm
ENISA	European Union Agency for Cybersecurity
EnWG	Energiewirtschaftsgesetz
EPEX	European Power Exchange

ERP	Enterprise Resource Planning
ETRM	Energy Trading and Risk Management
ETSI	European Telecommunications Standards Institute
EU	Europäische Union
EUCC	EU Common Criteria
EUCS	EU Cybersecurity Scheme
GAiN	Grundsätzliche Anforderungen im Nachweisverfahren
GIS	Geoinformationssystem
gMSB	Grundzuständiger Messstellenbetreiber
GPKE	Geschäftsprozesse zur Kundenbelieferung mit Elektrizität
GWA	Gateway-Administrator
IEC	International Electrotechnical Commission
IKT	Informations- und Kommunikationstechnologie
IP	Internet Protocol
IS-U	Industry Solution for Utilities
ISMS	Informationssicherheitsmanagementsystem
ISO	International Organization for Standardization
IT	Information Technology
ITIL	Information Technology Infrastructure Library
IT-SiKat	IT-Sicherheitskatalog
KBP	Konformitätsbewertungsprogramm
KPI	Key Performance Indicator
KRITIS	Kritische Infrastrukturen
kWh	Kilowattstunde
MDMS	Meter Data Management System
MsbG	Messstellenbetriebsgesetz
MUSS	Mindestanforderungen zur Umsetzung sicherer Systeme
MW	Megawatt
NIS2	Network and Information Security Directive 2

OFFIS	Oldenburger Forschungs- und Entwicklungsinstitut für Informatik-Werkzeuge und Systeme
OT	Operational Technology
PAM	Privileged Access Management
PE	Prüfelemente
PKI	Public Key Infrastructure
RED	Radio Equipment Directive
RTU	Remote Terminal Unit
SAP	Systeme, Anwendungen und Produkte in der Datenverarbeitung
SCADA	Supervisory Control and Data Acquisition
SLA	Service Level Agreement
SMGW	Smart Meter Gateway
SOLL	Sollwert
SPS	Speicherprogrammierbare Steuerung
SÜG	Sicherheitsüberprüfungsgesetz
TISAX	Trusted Information Security Assessment Exchange
TK	Telekommunikation
TKG	Telekommunikationsgesetz
TLS	Transport Layer Security
TR	Technische Richtlinie
TR-02102	Technische Richtlinie zur Kryptographischen Absicherung
TR-03109	Technische Richtlinie für Smart Meter Gateways
TR-03116	Technische Richtlinie für die elektronische Signatur
TR-03122	Technische Richtlinie für die sichere Identität
TR-03124	Technische Richtlinie für sichere E-Mail-Kommunikation
TR-03130	Technische Richtlinie für die sichere Videoüberwachung
VB	Verfahrensbeschreibung
VPN	Virtual Private Network
wMSB	Wettbewerblicher Messstellenbetreiber

Glossar

Begriff	Definition
Anomalieerkennung	Verfahren zur Identifikation von ungewöhnlichem oder verdächtigem Verhalten in IT-/OT-Systemen
Audit	Systematische Untersuchung, ob Prozesse oder Systeme festgelegte Anforderungen erfüllen
BSI-IT-Grundschutz	Methodisches Rahmenwerk des BSI zur systematischen Absicherung von IT-Systemen
Bundesamt für Sicherheit in der Informationstechnik (BSI)	Bundesbehörde für IT-Sicherheit in Deutschland, zuständig unter anderem für § 8a BSIG, KRITIS-Umsetzung und Technische Richtlinien
Bundesnetzagentur (BNetzA)	Nationale Regulierungsbehörde für den Energiesektor, zuständig für sicherheitsbezogene Nachweise gemäß § 11 EnWG
Bundesverband der Energie- und Wasserwirtschaft (BDEW)	Branchenverband der deutschen Energie- und Wasserwirtschaft, erarbeitet unter anderem branchenspezifische Sicherheitsstandards und Praxisleitfäden
Common Criteria (CC)	Internationaler Standard für die Sicherheitszertifizierung von IT-Produkten (ISO/IEC 15408), dient der Bewertung von Vertrauensniveaus sicherheitskritischer Komponenten
Cyber Resilience Act (CRA)	EU-Verordnung zu Sicherheitsanforderungen für digitale Produkte und Software, inklusive verpflichtender Produktzertifizierungen
Deutsche Akkreditierungsstelle (DAkkS)	Nationale Behörde zur Akkreditierung von Zertifizierungsstellen, die zum Beispiel ISO/IEC-27001-Audits durchführen
Energiewirtschaftsgesetz (EnWG)	Zentrales Gesetz zur Regulierung der Energieversorgung in Deutschland
European Common Criteria (EUCC)	Geplanter EU-Zertifizierungsrahmen für IT-Produkte basierend auf den Common Criteria
European Cybersecurity Scheme (EUCS)	Geplante EU-weite Zertifizierung für Cloud-Dienste gemäß EU Cybersecurity Act
Gateway-Administrator (GWA)	Verantwortlich für die sichere Konfiguration und den Betrieb von Smart Meter Gateways
Geltungsbereich	Der Umfang (z. B. Organisationseinheit, System), auf den sich eine Zertifizierung oder ein Audit bezieht
Hybrides Prüfmodell	Kombination formalisierter Zertifizierungen mit dialogischer, risikobasierter Prüfung
Hybridinfrastruktur (IT/OT)	Technologische Umgebung mit enger Verzahnung von IT-Systemen und operationalen Technologien
Informationssicherheitsmanagementsystem (ISMS)	System zur Planung, Umsetzung und kontinuierlichen Verbesserung von Informationssicherheit

Begriff	Definition
IT-Dienstleister	Unternehmen mit Aufgaben wie Hosting, Wartung oder Betrieb sicherheitskritischer Systeme
IT-Sicherheitsgesetz 2.0 (IT-SiG 2.0)	Erweiterung des BSIG mit neuen Pflichten für KRITIS-Betreiber, Herstellervorgaben und BSI-Kompetenzen
Komponentenhersteller	Hersteller sicherheitsrelevanter Hard- oder Softwarekomponenten
Konformitätsbewertungsprogramm (KBP)	Strukturierte Prüfsystematik der BNetzA zur Nachweiserbringung eines ISMS gemäß § 11 EnWG, regelt zum Beispiel Auditumfang, Nachweisdokumente und Auditorqualifikation
KRITIS-Betreiber	Betreiber Kritischer Infrastrukturen gemäß BSI-KritisV
KRITIS-Dachgesetz	Geplantes Gesetz zur sektoübergreifenden Regulierung Kritischer Infrastrukturen
Kritische Dienste	IT- oder OT-gestützte Services, die für Versorgungssicherheit oder Netzstabilität unerlässlich sind
Kritische Funktionen	Tätigkeiten, deren kontinuierliche Verfügbarkeit für versorgungsrelevante Aufgaben notwendig ist
Kritische Infrastruktur (KRITIS)	Anlagen oder Systeme mit großer Bedeutung für das Gemeinwesen
Kritische Komponenten	Technische Bauteile, deren Ausfall oder Kompromittierung wesentliche Auswirkungen haben kann
Kritische Prozesse	Prozesse, deren Störung zu erheblichen Versorgungs- oder Funktionsausfällen führen kann
Kritische Systeme	IT-/OT-Systeme, deren Ausfall die Betriebsfähigkeit Kritischer Infrastrukturen gefährdet
Lieferkette	Vorgelagerte Systeme, Produkte und Dienstleister mit sicherheitsrelevanten Funktionen
Messstellenbetriebsgesetz (MsbG)	Gesetzliche Grundlage für den Einsatz intelligenter Messsysteme
Modulare Zertifizierungsarchitektur	Nachweissystem mit aufeinander aufbauenden, gegenseitig anerkannten Prüfungen
Nachweis	Belege über die Umsetzung sicherheitsrelevanter Anforderungen, zum Beispiel durch Zertifikat oder Audit
Netzwerksegmentierung	Trennung von Netzwerkbereichen (z. B. IT und OT) zur Eindämmung von Angriffen
NIS2-Richtlinie	EU-Richtlinie zur Erhöhung des Cybersicherheitsniveaus kritischer Einrichtungen
Notfall- und Krisenmanagement	Strukturen und Prozesse zur Reaktion auf Sicherheitsvorfälle oder Betriebsstörungen
Patch- und Update-Planung	Systematische Aktualisierung zur Schließung von Sicherheitslücken
Prüfelemente (PE)	Vom BSI eingeführte Standardstruktur zur Dokumentation der Nachweise nach § 8a BSIG (PE.M = Maßnahmen, PE.R = Risiken, PE.A = Angemessenheit, PE.E = Erklärung)

Begriff	Definition
Prüfung	Fachliche Kontrolle im Rahmen von Zertifizierungen oder gesetzlichen Nachweisverfahren
Redispatch 2.0	Erweiterung der Redispatch-Regelungen in Deutschland zur netzdienlichen Steuerung auch kleinerer Erzeugungsanlagen, bringt neue Pflichten für Netzbetreiber und Anlagenbetreiber mit sich
Resilienz	Fähigkeit, trotz Störungen betriebsfähig zu bleiben und sich schnell zu erholen
Resilienzplan	Strategisches Konzept zur Sicherstellung kritischer Prozesse bei Störungen
Schulungs- und Sensibilisierungsmaßnahmen	Maßnahmen zur Erhöhung der Fachkompetenz und des Sicherheitsbewusstseins
Segmentierung (OT/IT)	Spezifische Trennung operationeller und informationstechnischer Systeme
Smart Meter Gateway (SMGW)	Sicherheitsrelevante Kommunikationseinheit im intelligenten Messsystem
Stand der Organisation	Reifegrad der Organisation in Bezug auf Prozesse, Strukturen und Sicherheitskultur
Stand der Technik	Anerkannter, aktueller Entwicklungsstand sicherheitsrelevanter Technologien
Technische Richtlinie (TR)	BSI-Vorgaben zur sicheren Gestaltung technischer Systeme
Verfügbarkeit (Schutzziel)	Sicherstellung der Nutzbarkeit von Informationen und Systemen bei Bedarf
Zertifizierung	Formelle Bestätigung, dass Systeme oder Produkte definierte Normanforderungen erfüllen
§ 8a BSIG	Verpflichtet Betreiber Kritischer Infrastrukturen zum Aufbau eines ISMS sowie zur Vorlage entsprechender Nachweise beim BSI
§ 11 EnWG	Paragraf im Energiewirtschaftsgesetz, der die Einführung eines ISMS und Nachweise zur IT-Sicherheit verlangt, auch unterhalb der KRITIS-Schwelle

Ein Projekt der

dena

www.dena.de

future-energy-lab.de