Deloitte.

Together makes progress

Cybersicherheit im Fokus

Regulatorischer Wandel als strategische Herausforderung für Energieversorger

Energieversorger stehen zunehmend im Fokus geopolitischer Spannungen und Cyberangriffe. Parallel dazu steigen die regulatorischen Anforderungen durch EU-Richtlinien wie NIS2 und nationale Gesetze. Die überarbeiteten IT-Sicherheitskataloge (SiKat) legen verstärktes Augenmerk auf OT-Sicherheit, Business Continuity und Resilienz. Dieses Whitepaper zeigt, wie Energieunternehmen diesen Herausforderungen systematisch begegnen und ihre Cyberresilienz stärken können.

Bedrohungslage: Cyberangriffe auf dem Vormarsch

Die geopolitische Lage hat Energieinfrastrukturen ins Zentrum sicherheitspolitischer Bedrohungen gerückt. Angriffswellen auf europäische Netzbetreiber im Jahr 2024, die zu massiven Störungen und Preissprüngen führten, und die Sprengung der Nord-Stream-Pipelines verdeutlichen: Kritische Energieinfrastrukturen sind strategische Angriffsziele geworden.

Parallel zu physischen Angriffen tobt der Cyberkrieg. Die zahlreichen Störungen und Sabotageaktionen der letzten Jahre legen eine Verbindung zu politischen Akteuren und Nationalstaaten nahe und demonstrieren damit die neue Dimension moderner Cyberbedrohungen. Die Statistiken sprechen eine klare Sprache:

- **Explosionsartiger Anstieg:** 80 Prozent mehr Cyberangriffe auf Energieunternehmen
- **Klarer Fokus:** 11 Prozent aller weltweiten Cyberangriffe zielen auf den Energiesektor
- **Geografische Schwerpunkte:** Die USA und Europa stehen besonders im Visier

Die Entwicklung zeigt einen beunruhigenden Trend:
Was 2010 mit Stuxnet als isoliertem Angriff auf Industrieanlagen begann, ist heute zur systematischen Bedrohung kritischer Infrastrukturen geworden. State-Driven Actors verfolgen strategische Interessen und verfügen über erhebliche Ressourcen.

Technologische Realität: die IT/OT-Konvergenz als zentrale Herausforderung

Die fortschreitende Verschmelzung von IT und OT (IT/OT-Konvergenz) bringt neue Risiken mit sich. Während für IT-Systeme vielerlei Schutzmaßnahmen möglich sind, bleiben viele OT-Komponenten veraltet und sind nicht auf moderne Sicherheitslösungen wie Endpoint Detection & Response (EDR) oder automatisierte Patchprozesse ausgelegt.

Die Verschmelzung von IT und OT führt zu zusätzlichen Herausforderungen:

- **Hybride IT-Landschaften** mit Cloud- und On-Premise-Komponenten
- **Mangelnde Standardisierung** und eingeschränkte Automatisierungsmöglichkeiten
- **Hohe Komplexität** bei der Integration sicherheitsrelevanter Prozesse

Regulatorischer Wandel: neue Verantwortung für Energieversorger

Staatliche Behörden weltweit haben die zunehmende Bedeutung von Cybersicherheit im Energiesektor erkannt und auch in Europa und Deutschland mit einer Reihe gezielter regulatorischer Maßnahmen reagiert.

EU-Ebene

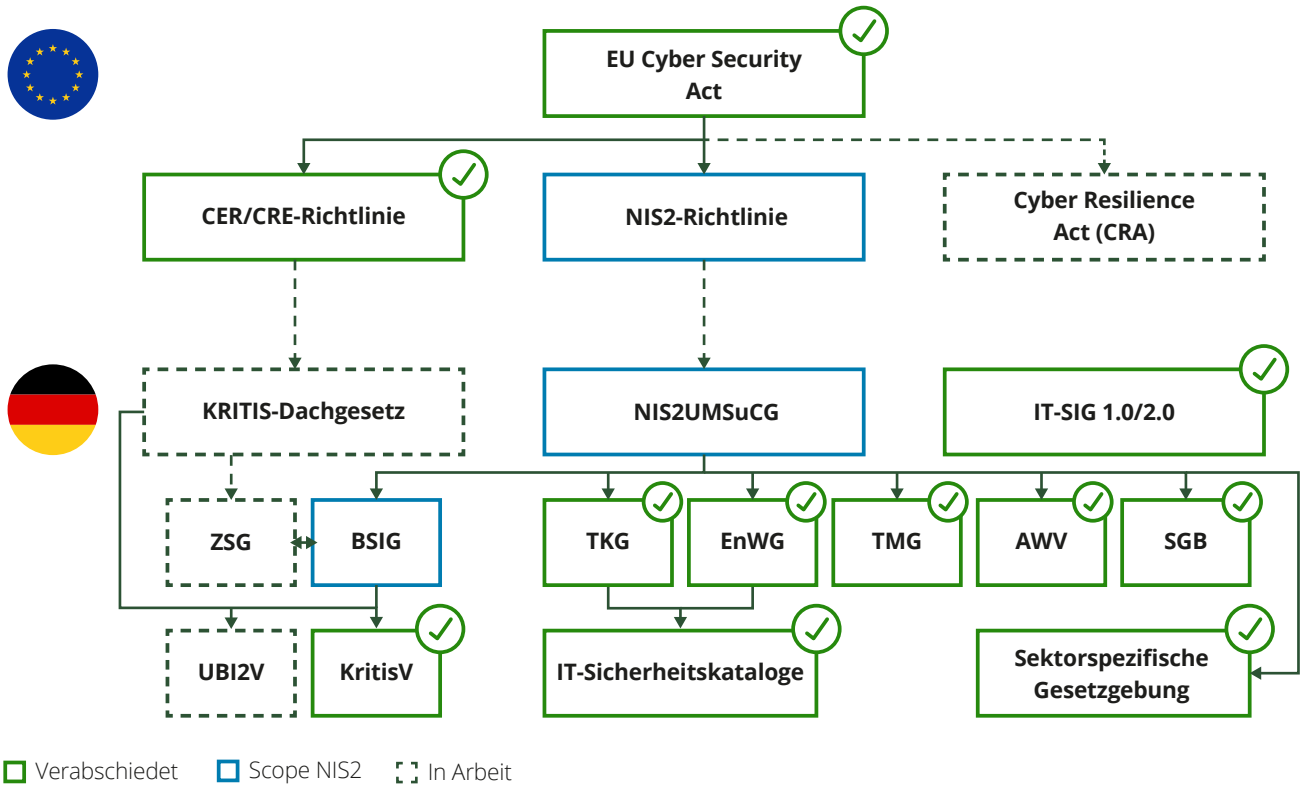
- **EU Cyber Security Act (CSA):** Zertifizierungsrahmen für IKT-Produkte seit 2019
- **NIS2-Richtlinie:** Deren Umsetzung bringt neue Anforderungen wie ein verpflichtendes Risikomanagement, technische Schutzmaßnahmen sowie umfassende Meldepflichten bei Sicherheitsvorfällen
- **CER/CRE-Richtlinie:** physische Sicherheit kritischer Infrastrukturen
- **Cyber Resilience Act:** Cybersicherheitsstandards für digitale Produkte

Deutsche Umsetzung

- **NIS2-Umsetzungsgesetz (NIS2UmsuCG):** nationale Implementierung der EU-Vorgabe
- **KRITIS-Dachgesetz:** Umsetzung der CER/CRE-Richtlinie
- **Energiewirtschaftsgesetz (EnWG):** branchenspezifische Regelungen
- **IT-Sicherheitskataloge (SiKat):** operative Anforderungen der Bundesnetzagentur

Für Energieversorger ergibt sich daraus ein komplexes Spannungsfeld: Sie müssen gleichzeitig technologische Modernisierung vorantreiben, hohe Sicherheitsstandards erfüllen und den wachsenden regulatorischen Anforderungen gerecht werden. Die zentrale Herausforderung besteht darin, diese drei Dimensionen – Digitale Transformation, Sicherheit und Compliance – in Einklang zu bringen, ohne die operative Stabilität zu gefährden.

Abb. 1 – Cybersicherheitsregulatorik



IT-Sicherheitskatalog im Wandel: Von OT-Sicherheit zu Resilienz und BCM

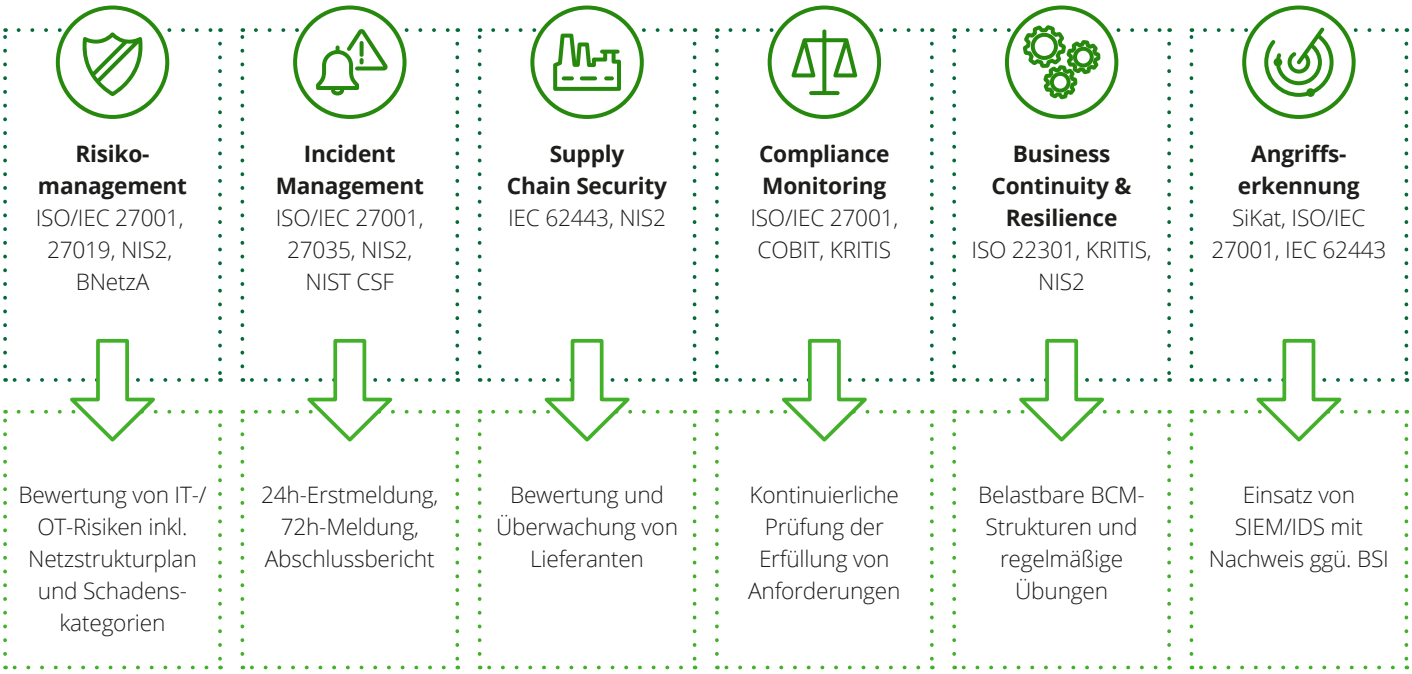
Neuer Fokus auf OT-Sicherheit

Die Bundesnetzagentur überarbeitet seit Mai 2025 die SiKat im Rahmen einer Konsultation, um den neuen Anforderungen aus NIS2 und dem KRITIS-Dachgesetz Rechnung zu tragen. Dabei rücken erstmals systematisch OT-Sicherheit, Business Continuity und physische Resilienz in den Fokus.

Zentrale Änderungen

- Erweiterte Risikoanalysen für IT/OT-Systeme
- Verschärfte Meldepflichten bei Cybervorfällen (24h-Erstmeldung, 72h-Folgemeldung, Abschlussbericht (NIS2))
- Neue Anforderungen an Lieferkettenmanagement
- Verstärkte Schulungspflichten für Führungskräfte und erhöhte persönliche Verantwortung/Haftung der Unternehmensleitung (NIS2)
- Einführung eines Business-Continuity-Managements (BCM) als Pflichtbestandteil
- Anwendung eines Allgefahren-Ansatzes (nicht nur Cyber, auch Naturgefahren, Ausfälle, physische Risiken)
- Konsolidierung der bisher getrennten Kataloge (Stromnetz, Gasnetz, Energieanlagen)

Abb. 2 – Unmittelbare Handlungsfelder für Betreiber kritischer Energieinfrastruktur



Synergien nutzen
Die parallele Umsetzung von NIS2, EnWG-Anforderungen und den SiKat der BNetzA ermöglicht Effizienzgewinne durch koordinierte Umsetzung.

Bewährte Standards als Fundament
NIS2, KRITIS und die SiKat stützen sich überwiegend auf etablierte internationale Standards.

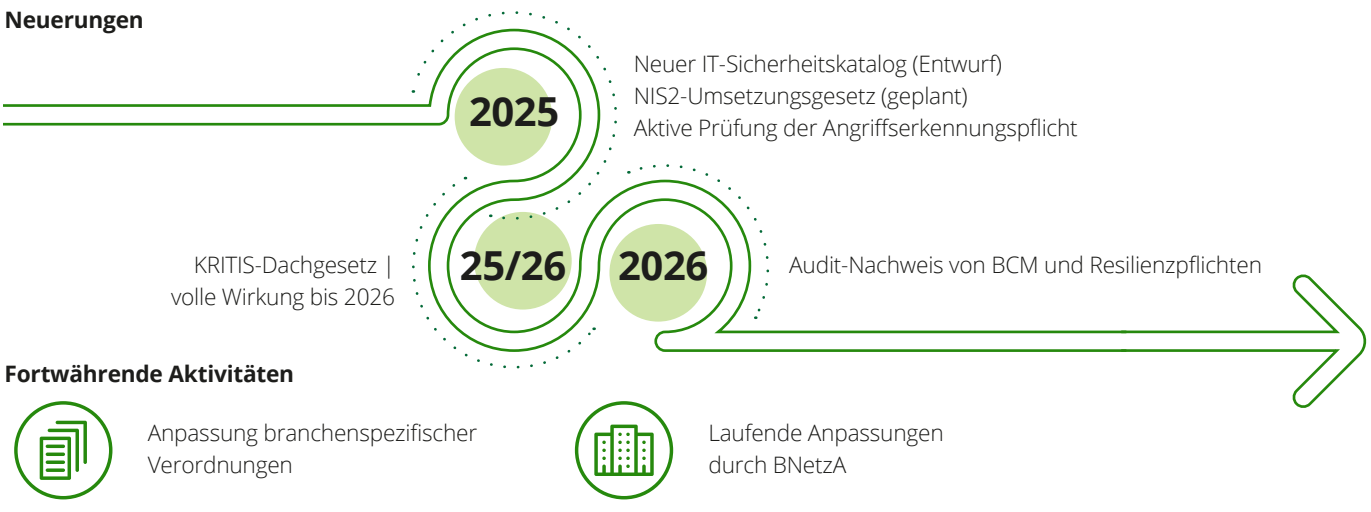
- **ISO/IEC 27001:2022:** Basis für ISMS-Anforderungen in allen Regulatorien
- **NIST Cybersecurity Framework:** strukturierter Ansatz für Risiko- und Incident-Management
- **IEC 62443:** Standard für OT-Sicherheit in Industrie- und Steuerungssystemen
- **COBIT:** Referenzmodell für IT-Governance und -Management
- **ISO 22301 (Business-Continuity-Management):** Rahmenwerk für das BCM
- **DIN EN ISO/IEC 27019:** spezifische Ergänzung für Energie- und Prozessleitsysteme

Zeitplan der regulatorischen Umsetzung

- **Ab 2025:** Angriffserkennungspflicht wird aktiv geprüft und auditiert (seit 2023 gesetzlich verankert)
- **2025:** Konsultationsphase und Entwurf des neuen, konsolidierten SiKat
- **2025:** geplante Verabschiedung des NIS2-Umsetzungsgesetzes (verzögert durch Regierungswechsel)
- **2025/2026:** schrittweise Umsetzung des KRITIS-Dachgesetzes ab 2025, volle Wirksamkeit plausibel bis 2026
- **Ab 2026:** vollständiger Nachweis von BCM- und Resilienzpflichten im Audit
- **Kontinuierlich:** Anpassung branchenspezifischer Verordnungen
- **Fortwährend:** Anpassungen durch BNetzA

Die regulatorische Verdichtung führt zu Überschneidungen und kann bei unkoordinierter Umsetzung zu erheblichen Mehrkosten führen. Die neue Prozessorientierung, die Pflicht zur Resilienzplanung sowie Aspekte wie Asset-Transparenz, Managementhaftung und Krisenübungen verdeutlichen, dass der SiKat zunehmend als Gesamtresilienzrahmen verstanden wird – nicht mehr nur als klassisches IT/OT-Sicherheitsinstrument.

Abb. 3 – Zeitplan der regulatorischen Umsetzung



Vom Risiko zur Resilienz: Deloittes Toolbox für Energieversorger

Deloitte hat gemeinsam mit Energieversorgern eine modulare, ganzheitliche Lösung entwickelt, die regulatorische Anforderungen mit operativer Widerstandsfähigkeit verbindet. Der Ansatz bildet die End-to-End-Journey eines IT/OT-Sicherheitsprogramms ab – von der ersten Risikoanalyse bis zum nachhaltigen Betriebsmodell. Besondere Berücksichtigung finden die Anforderungen der Energiebranche sowie relevante Standards wie NIS2, KRITIS, EnWG, ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27019 und IEC 62443.

Dank umfangreicher Projekterfahrung – von der Absicherung von Windparks bis hin zur Entwicklung von OT-Sicherheitsarchitekturen – unterstützt Deloitte Energieversorger bei der Umsetzung moderner Sicherheitskonzepte.

Die Grundlagen unserer Strategie:

- Security-by-Design
- Zero-Trust-Prinzipien
- Defense-in-Depth
- Monitoring und angepasste Endpoint-Security-Lösungen

Ergänzend tragen Services wie Managed SOC, Incident Response Support und Awareness-Kampagnen dazu bei, eine schnelle und effektive Angriffsdetektion und -abwehr (Threat Intelligence & Hunting) sowie eine resiliente Sicherheitskultur zu gewährleisten.

Deloitte begleitet Versorger dabei von der Strategieentwicklung bis in den dauerhaften Betrieb.

Abb. 4 – Phasen des IT/OT-Sicherheitsprogramms

	Step 1 **Assessment & Gap Analysis**	Step 2 **Governance Setup**	Step 3 **Implementation & Remediation**	Step 4 **Operate & Improve**
OT Activities	• Determine/Analyse OT Standard Way of Working • Align compliance requirements • Map IT/OT assets & dependencies • Perfom risk assessment	• Defining future Target Operating Model (TOM) • Defining policies and procedures • Creating technical solution architecture • Establish Management buy-in	• Pilot blueprints in dedicated locations and areas • Rollout field-tested solution architecture • Implement TOM with defined roles and responsibilities	• Identify KPI/KRI in sustainably measure and report security posture • Introduce regular assessments or audits • Identify and prioritize future improvements based on KPI/KRI in the form of a continuous improvement process
Challenges	• Incomplete documentation and tooling • Lack of visibility into OT assets • Unclear responsibilities • Regulatory frameworks misaligned with reality	• Strictly IT-driven operating model • Heterogeneous OT technology and infrastructure (legacy assets, flat networks) • Lack of OT roles and expertise • Lack of management support	• Tailor solutions to local requirements • Generalize tailoring to fit into other locations • Acquire downtimes to introduce technical solutions • Translate TOM to company culture	• KPI/KRI and reporting overload • False sense of security • Inefficient transition from project to regular operations • Alert fatigue
Outputs	• Compliance gap report • IT/OT risk reduction roadmap • Effort & cost calculation	• Governance, compliance & TOM documents • Blueprints for scalable technical rollout • Implementation roadmap	• Introduction of security solutions to reduce risk • First gains in efficiency and transparency due to TOM implementation	• Continous Improvement established • KPI/KRI-driven unified reporting • Optimized IT/OT baselines
Compliance	**Assess Compliance** Review regulations and technical requirements to identify key gaps	**Define Compliance Framework** Set governance, roles, policies and technical architecture for IT/OT	**Implement Compliance** Apply controls, tools and integrate into operations	**Sustain Compliance** Monitor continuously, track KPIs, and perform audits

Fazit und Handlungsempfehlungen

Die neue regulatorische Landschaft in der Cybersicherheit stellt Energieversorger vor erhebliche Herausforderungen, bietet aber auch Chancen für eine systematische Stärkung der Cyberresilienz.

Erfolgsfaktoren

- **Frühzeitige Planung:** Rechtzeitige Vorbereitung auf regulatorische Deadlines
- **Integrierte Ansätze:** Koordinierte Umsetzung verschiedener Compliance-Anforderungen
- **Risikoorientierung:** Systematischer Fokus auf kritische Assets sowie deren Bedrohungen und Schwachstellen – in einem integrierten System, das IT-, OT- und regulatorische Managementbereiche verbindet
- **Kontinuierliche Verbesserung:** Aufbau adaptiver Sicherheitsarchitekturen

Effizienzfaktoren

Die Komplexität der regulatorischen Landschaft und die kritische Bedeutung der Energieinfrastruktur erfordern spezialisierte Expertise. Erfolgreiche Unternehmen setzen zur Durchführung eines schlanken und zielgerichteten Programms auf:

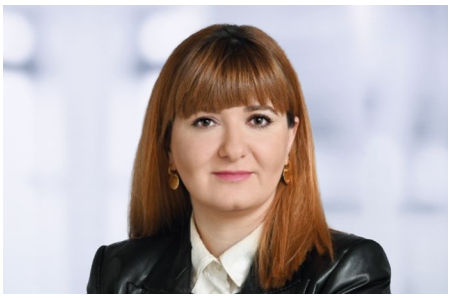
- **Regulatorische Expertise:** Fundiertes Verständnis relevanter gesetzlicher, normativer und branchenspezifischer Anforderungen
- **Technische Kompetenz:** Praktische Erfahrung in der Umsetzung von Sicherheitsmaßnahmen in IT- und OT-Umgebungen
- **Branchen-Know-how:** Spezifisches Verständnis der Herausforderungen in der Energiewirtschaft
- **Umsetzungserfahrung:** Bewährte Methoden und Tools

Über Deloitte Cyber

Deloitte Cyber ist führender Anbieter von Cybersecurityberatung. Unsere Spezialisten unterstützen Unternehmen dabei, ihre digitale Transformation sicher zu gestalten. Unser Fokus auf kritische Infrastrukturen und unsere langjährige Erfahrung in der Energiewirtschaft machen uns zum vertrauenswürdigen Partner für die Herausforderungen der Energiewende.

Kontakte

Fabian Mihailowitsch
Partner | Cyber
Technology & Transformation
Tel: +49 89 29036 6998
fmihailowitsch@deloitte.de



Tamara Okropiridze
Senior Manager | Cyber
Technology & Transformation
Tel: +49 69 75695 7215
tokropiridze@deloitte.de

Daniel Götz
Senior Manager | Cyber
Technology & Transformation
Tel: +49 911 23074 247
dagoetz@deloitte.de

Deloitte.

MAKING AN IMPACT THAT MATTERS since 1845

Stand 11/2025