IT-Sicherheit und Cyberresilienz in kritischen Infrastrukturen

IT-Sicherheit und Cyberresilienz in kritischen Infrastrukturen

Einleitung und Kontextualisierung

Die Gewährleistung der Versorgungssicherheit in modernen Volkswirtschaften hängt untrennbar von der Integrität und Verfügbarkeit ihrer kritischen Infrastrukturen (KRITIS) ab. Im Zuge der digitalen Transformation des Energiesektors – oft subsumiert unter dem Begriff "Smart Grid" – vollzieht sich ein fundamentaler Wandel von isolierten, analogen Betriebsumgebungen hin zu hochvernetzten, IP-basierten Systemarchitekturen. Diese Konvergenz von Informationstechnologie (IT) und operativer Technologie (OT) eröffnet zwar enorme Effizienzpotenziale und ist für die Integration volatiler erneuerbarer Energien unumgänglich, sie exponiert die einst geschlossenen Systeme jedoch gegenüber einer volatilen Cyber-Bedrohungslage.

Die Absicherung dieser Infrastrukturen erfordert daher einen Paradigmenwechsel: weg von rein präventiven Schutzmaßnahmen hin zu einer umfassenden Cyberresilienz. Dieser Beitrag analysiert die spezifische Bedrohungslage für digitalisierte Energienetze, bewertet den aktuellen Stand der Digitalisierung als Sicherheitsfaktor und definiert Anforderungen an Information Security Management Systems (ISMS) im Kontext regulatorischer Vorgaben.

Analyse der Bedrohungslage für digitalisierte Energienetze

Die Bedrohungslandschaft für Energieversorgungsunternehmen (EVU) und Netzbetreiber hat sich diversifiziert. Während physische Angriffe und Naturkatastrophen traditionelle Risikoszenarien darstellten, dominieren heute Advanced Persistent Threats (APTs), Ransomware-Kampagnen und Supply-Chain-Angriffe die Risikobewertung.

Konvergenz von IT und OT als Risikotreiber

Historisch betrachtet waren Netzleitsysteme durch das "Air-Gap"-Prinzip physisch vom öffentlichen Internet und der Unternehmens-IT getrennt. Mit der Einführung von Fernwartungszugängen, intelligenten Messsystemen (Smart Meter Gateways) und der IoT-basierten Überwachung von Ortsnetzstationen erodiert diese Trennung. Angreifer können laterale Bewegungen nutzen, um von kompromittierten Office-Netzwerken in kritische Steuerungsnetze (SCADA/ICS) vorzudringen.

Ein spezifisches Risiko ergibt sich aus der Dezentralisierung der Erzeugungsstruktur. Eine Vielzahl kleiner Einspeiser (Photovoltaik, Windkraft) kommuniziert mit dem Netzbetreiber. Jede dieser Schnittstellen stellt einen potenziellen Vektor für Cyberangriffe dar. Werden diese Endpunkte nicht adäquat gehärtet, könnten Botnetze theoretisch Tausende von Wechselrichtern manipulieren, um Instabilitäten in der Netzfrequenz zu provozieren.

Stagnation der Digitalisierung als Vulnerabilität

Paradoxerweise stellt nicht nur die fortschreitende Vernetzung, sondern auch die *stockende* Modernisierung ein Sicherheitsrisiko dar. Veraltete Legacy-Systeme, für die keine Sicherheitsupdates mehr verfügbar sind, verbleiben länger im Netz als geplant.

Aktuelle Untersuchungen zur Digitalisierung der Verteilnetze im DACH-Raum deuten auf eine bedenkliche Stagnation hin. Eine gemeinsame Studie von envelio und energate aus dem Jahr 2025 zeigt auf, dass die Digitalisierung in den Verteilnetzen kaum voranschreitet, gebremst durch interne Hürden und einen geringen Automatisierungsgrad[^1]. Diese Verzögerung hat direkte sicherheitstechnische Implikationen:

1. **Mangelnde Sichtbarkeit:** Ohne durchgängige Digitalisierung fehlt Netzbetreibern die Echtzeit-Transparenz über den Netzzustand (Observability), was die Erkennung von

Anomalien und Cyberangriffen erschwert.
2. **Fehlende Automatisierung:** Die Studie hebt hervor, dass manuelle Prozesse dominieren. Im Falle eines Cyberangriffs ist eine manuelle Reaktion ("Incident Response") oft zu langsam, um Kaskadeneffekte zu verhindern. Automatisierte Abwehrmechanismen (z.B. automatische Netzsegmentierung) setzen einen hohen Digitalisierungsgrad voraus.

Siehe auch: Automatisierungstechniken in der Mittelspannungsebene

Strategien zur Erhöhung der Cyberresilienz

Während sich die klassische IT-Sicherheit (Cyber Security) auf die Abwehr von Angriffen konzentriert (Prävention), fokussiert die Cyberresilienz auf die Fähigkeit eines Systems, trotz eines erfolgreichen Angriffs oder Teilausfalls funktionsfähig zu bleiben oder den Normalzustand schnellstmöglich wiederherzustellen (Recovery und Continuity).

Resilience by Design in der Netzarchitektur

Für kritische Infrastrukturen ist der Ansatz der "Resilience by Design" essenziell. Dies beinhaltet redundante Kommunikationswege, segmentierte Netzwerkarchitekturen (Zonierung nach IEC 62443) und dezentrale Steuerungslogiken, die auch bei Ausfall der zentralen Leittechnik einen Notbetrieb (Inselbetrieb) ermöglichen.

Die Rolle von Energiespeichersystemen (BESS) für die Systemstabilität

Ein oft unterschätzter Faktor für die Resilienz gegenüber Cyberangriffen ist die physische Pufferung des Netzes. Battery Energy Storage Systems (BESS) spielen hierbei eine Schlüsselrolle. Sie können Frequenzschwankungen, die durch manipulierte Einspeiser oder Lastabwürfe entstehen, kurzfristig kompensieren und so einen Blackout verhindern, während IT-Sicherheitsteams den Angriff isolieren.

Im Jahr 2025 profitiert das deutsche Stromnetz zunehmend von der Integration großformatiger Speicherlösungen. Diese Technologien sind nicht nur für die Energiewende relevant, sondern dienen als stabilisierendes Element im Sinne der Versorgungssicherheit gemäß

Energiewirtschaftsgesetz (EnWG)[^2]. Die Fähigkeit von BESS, Systemdienstleistungen wie Primärregelleistung bereitzustellen, erhöht die Trägheit des Systems und gibt den Betreibern wertvolle Zeit zur Reaktion auf Cyber-Vorfälle. Die regulatorische Rahmensetzung durch die Bundesnetzagentur spielt hierbei eine entscheidende Rolle, um Anreize für den Einsatz solcher resilienzsteigernden Technologien zu schaffen.

Siehe auch: Netzstabilisierung durch leistungselektronische Systeme

Anforderungen an ISMS in der Energiewirtschaft

Um den komplexen Bedrohungen systematisch zu begegnen, schreibt der Gesetzgeber für Betreiber kritischer Infrastrukturen die Implementierung eines Information Security Management Systems (ISMS) vor. In Deutschland bildet das IT-Sicherheitsgesetz 2.0 (und in der Folge die Umsetzung der NIS-2-Richtlinie) den rechtlichen Rahmen.

Spezifika der ISO/IEC 27019

Während die ISO/IEC 27001 den allgemeinen Standard für ISMS definiert, konkretisiert die ISO/IEC 27019 die Anforderungen für die Prozessleittechnik in der Energieversorgung. Ein KRITIS-konformes ISMS muss folgende Kernaspekte abdecken:

1. **Asset Management:** Vollständige Inventarisierung aller IT- und OT-Komponenten (Hardware, Software, Firmware-Stände). Wie die Studie zur Verteilnetz-Digitalisierung andeutet, ist dies aufgrund der stagnierenden Automatisierung oft noch eine manuelle und fehleranfällige Aufgabe[^1].
2. **Risikomanagement:** Zyklische Bewertung von Bedrohungsszenarien unter Berücksichtigung der physikalischen Auswirkungen (z.B. Personenschaden, Versorgungsausfall).
3. **Lieferantenmanagement:** Überprüfung der Sicherheit in der Lieferkette (Supply Chain Security), insbesondere bei Wartungsdienstleistern und Software-Zulieferern.
4. **Incident Management und Meldewesen:** Etablierung von Meldewegen an nationale Behörden (z.B. BSI) und Integration in branchenspezifische Warnsysteme (UP KRITIS).

Regulatorische Treiber und Compliance

Das Energiewirtschaftsgesetz (EnWG) verpflichtet Betreiber von Energieversorgungsnetzen, einen angemessenen Schutz gegen Bedrohungen für die Telekommunikations- und EDV-Systeme zu gewährleisten, die für einen sicheren Netzbetrieb notwendig sind. Die Bundesnetzagentur hat

hierzu in Abstimmung mit dem BSI einen Sicherheitskatalog erstellt[^3]. Die Einhaltung dieser Vorgaben muss regelmäßig durch Audits nachgewiesen werden.

Die Integration moderner Technologien wie BESS in das Netzmanagement erfordert zudem eine Anpassung der Sicherheitskonzepte, da diese Speicher selbst über digitale Schnittstellen gesteuert werden und somit Teil der kritischen Angriffsfläche werden[^2]. Ein ISMS darf daher nicht statisch sein, sondern muss als "lebendes System" mit der technologischen Entwicklung (z.B. Cloud-Integration, KI im Netzbetrieb) mitwachsen.

Fazit und Ausblick

Die Cyberresilienz kritischer Infrastrukturen ist kein rein technisches Problem, sondern eine strategische Notwendigkeit für die nationale Sicherheit. Die Analyse zeigt, dass die Bedrohungslage durch die zunehmende Vernetzung steigt, während interne Hürden bei der Digitalisierung die Implementierung automatisierter Schutzmaßnahmen hemmen.

Erfolgreiche Sicherheitsstrategien müssen daher dual ansetzen: Zum einen muss die digitale Transformation der Verteilnetze beschleunigt werden, um Transparenz und Reaktionsfähigkeit zu erhöhen. Zum anderen müssen physische Resilienzfaktoren, wie der Einsatz von Großbatteriespeichern, in das Sicherheitskonzept integriert werden. Nur durch die Verschmelzung von robustem ISMS, moderner Netztechnologie und regulatorischer Compliance kann die Versorgungssicherheit in einer digitalisierten Energiewelt gewährleistet werden.

Quellenverzeichnis

[^1]: Solarserver. (2025). *Verteilnetz-Digitalisierung stagniert: Neue Studie von envelio und energate 2025*. Studie zur Digitalisierung der Verteilnetze im DACH-Raum, die interne Hürden und geringe Automatisierung bei Netzbetreibern aufzeigt.

[^2]: PwC. (2025). *Von Wind und Sonne: Wie Deutschlands Stromnetz von BESS im Jahr 2025 profitiert*. Blogbeitrag zur Bedeutung von Battery Energy Storage Systems (BESS) für das Stromnetz, Regulierung und Versorgungssicherheit.

[^3]: Bundesnetzagentur. (2025). *Sicherheitskatalog gemäß § 11 Absatz 1a Energiewirtschaftsgesetz (EnWG)*. (Kontextuelle Referenz basierend auf den regulatorischen Schlagwörtern der verwendeten Quellen). Vorgaben für die IT-Sicherheit von Energieversorgungsnetzen.

□□ Powered by STROMDAO KI

Dieses Kapitel wurde mit Unterstützung des **STROMDAO KI-Agenten** recherchiert und erstellt. Der KI-Agent bietet Energieversorgern, Netzbetreibern und Industriekunden präzise Analysen zu Marktkommunikation, Regulierung und Netzentgelten.

□□ Weiterführende Ressourcen zu diesem Thema

- **iMSys-Rollout-Prozess** – Praxisleitfaden zum Rollout intelligenter Messsysteme nach MsbG.
- **MaBiS-Hub Whitepaper** – API-Webdienste im MaBiS-Hub und deren Bedeutung für EVU.
- **§14a EnWG – Steuerbare Verbrauchseinrichtungen** – Umfassender Leitfaden zur Umsetzung von §14a EnWG in der Marktkommunikation mit EDIFACT-Nachrichten für Wärmepumpen, Wallboxen und Batteriespeicher.

□□ Weitere Informationen

- **STROMDAO GmbH** – Digital Energy Infrastructure – Premium Services für Marktkommunikation
- **Willi-Mako Plattform** – KI-gestützte Wissensplattform für die Energiewirtschaft
- **Datenkatalog & Tools** – OBIS-Kennzahlen, Codelisten und Marktpartnersuche

□□ 7 Tage kostenlos testen

Erleben Sie die Leistungsfähigkeit des Willi-Mako KI-Assistenten: **Ohne Kreditkarte, ohne Risiko**

Revision #1
Created 21 November 2025 14:11:19 by Thorsten Zoerner
Updated 21 November 2025 14:11:19 by Thorsten Zoerner