Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Positionspapier: Cybersicherheit im Energiesektor Deutschlands

1 Energieversorgung als Rückgrat unserer Gesellschaft

Die Energiesicherheit ist eine tragende Säule der nationalen Sicherheitsarchitektur. Mit der fortschreitenden Digitalisierung und Dezentralisierung des deutschen Energiesektors – insbesondere durch den massiven Ausbau erneuerbarer Energien – nimmt die Angriffsfläche für Cyberbedrohungen erheblich zu. Gleichzeitig ist die zuverlässige Stromversorgung ein kritischer Faktor für nahezu alle Bereiche des gesellschaftlichen Lebens, von Krankenhäusern über Verkehr bis hin zur Trinkwasserversorgung. Die aktuelle Bedrohungslage zeigt, dass staatliche und nichtstaatliche Akteure verstärkt versuchen, Schwachstellen im Energiesystem auszunutzen. Dieses Positionspapier formuliert zentrale Herausforderungen und Handlungsfelder für eine robuste Cybersicherheitsstrategie im deutschen Energiesektor.

2 Cybersicherheitslage: Eine angespannte Bedrohungssituation

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) stuft die Bedrohungslage im Bereich Kritischer Infrastrukturen (KRITIS) seit Jahren als „hoch“ ein. Der Energiesektor steht dabei besonders im Fokus von:

- Staatlich unterstützten Cyberoperationen (z. B. Russland, China, Iran, Nordkorea), die auf Destabilisierung und Spionage abzielen.
- Cyberkriminellen Gruppen, die Ransomware einsetzen und gezielt Energieunternehmen erpressen.
- Hacktivisten, die ideologische Ziele verfolgen, etwa im Kontext von Klima-/Energiepolitik.

3 Neue Herausforderungen im Kontext der Energiewende

Die Energiewende bringt notwendige strukturelle Veränderungen mit sich, durch die sich jedoch eine geänderte IT-Sicherheitsbedrohungslage ergibt:

- Dezentralisierung: Tausende kleinere Akteure wie private Haushalte mit Photovoltaikanlagen werden Teil des Energiesystems, oftmals ohne professionelle IT-Sicherheit und entsprechende Regulierung.
- Intelligente Netze und digitale Steuerungssysteme: Smart Grids, digitale Zähler (Smart Meter) und ferngesteuerte Anlagen eröffnen neue Angriffsmöglichkeiten
- Sektorkopplung: Die zunehmende Integration von Strom, Industrie und Verkehrssystemen erhöht die systemische Komplexität und Verwundbarkeit.

4 Neue Angriffsvektoren und Schwachstellen

Mit der Digitalisierung entstehen neue Einfallstore für Angreifer:

- Supply-Chain-Angriffe auf Software und Hardware von Energieanlagen (z. B. Solarwechselrichter, Netzleittechnik).
- Manipulation von Energieinfrastruktur durch Hersteller oder Dritte (z.B. Wechselrichter oder Smart Meter und deren Kommunikationsschnittstellen).
- Zero-Day-Exploits in industriellen Steuerungssystemen (ICS) und SCADA-Umgebungen.

- IoT-basierte Botnetze, die über schlecht gesicherte Endgeräte Angriffe auf Energienetze koordinieren.

5 Systemische Risiken für die Versorgungssicherheit

Ein erfolgreicher Cyberangriff kann weitreichende Folgen haben:

- Stromausfälle (Blackouts) im europäischen Verbundnetz durch gezielte Angriffe auf Netzleittechnik, virtuelle Kraftwerke oder über das Internet zugängliche private Energieanlagen (Wechselrichter, Wallboxen, Wärmepumpen usw.). Der Vorfall auf der iberischen Halbinsel – welcher gleichermaßen auch durch Cyber-Ursachen hätte entstehen können – verdeutlicht die Tragweite der Auswirkungen eines Stromausfalls.
- Versorgungsengpässe durch die Stilllegung dezentraler Einspeiser.
- Störungen der Notfall- und Kriseninfrastruktur, etwa in Krankenhäusern oder Telekommunikationsnetzen.

6 Notwendige Maßnahmen

a) Stärkung des BSI als zentrale Cybersicherheitsinstanz

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) steht mit seiner Expertise bereit, die zentrale Steuerungsrolle für die Cybersicherheit im Energiesektor zu übernehmen – als Vorgabengeberin und Koordinationsstelle. Um diese Aufgabe wirkungsvoll umsetzen zu können, braucht es:

- Horizontal einheitliche Anforderungen in allen KRITIS-Sektoren und darauf aufbauend klare Vorgaben für alle Akteure im Energiesystem, auch für kleinere Betreiber.
- Entwicklung und Durchsetzung einheitlicher, sektorspezifischer Sicherheitsstandards für alle Akteure – von Netzbetreibern bis zu dezentralen Anlagen.
- Ausbau der aufsichtsrechtlichen Befugnisse des BSI, inklusive Interventionskompetenzen bei Cyber-Vorfällen.
- Außerhalb der KRITIS-Sektoren muss die Cybersicherheit von Anlagen durch europäisch anschlussfähige präventive Standards, sektorspezifische Kontrollschichten sowie eine effektive Marktüberwachung sichergestellt werden.

b) Technische Standards und Resilienzmaßnahmen

Das BSI greift auf eine sektorübergreifende langjährige Expertise zurück und kann somit einen wertvollen Beitrag bei der Erarbeitung von technischen Standards leisten. Notwendig ist ein dreistufiger Sicherheitsansatz für technische Resilienz:

1. Basisabsicherung der gesamten operativen Infrastruktur (OT/IT-Netze, Kommunikationsschnittstellen).
2. Zielgerichtete Härtung zentraler Komponenten (z. B. Netzleittechnik, virtuelle Kraftwerke, Smart-Meter-Gateway-Infrastruktur mit hoheitlicher PKI, Speicher, Wechselrichter).
3. Hochsichere Absicherung exponierter Systeme mit hohem Schadenspotenzial (z. B. Netzkoppelpunkte, Steuerzentralen, zentrale Kontrollsysteme).

- Förderung von Redundanz- und Notfallkonzepten, insbesondere bei dezentralen Anlagen.
- Einsatz von fortschrittlicher Angriffserkennung (SIEM, IDS/IPS) in Netzleitstellen.

c) Kooperation und Informationsaustausch

- Ausbau der Zusammenarbeit zwischen Energieunternehmen, BSI, CERTs und Sicherheitsbehörden.
- BSI als zentrale Anlaufstelle für Bedrohungsanalyse, Frühwarnung und sektorübergreifende IT-Lagebilder.
- Enge Einbindung des BSI, u.a. über klare Zuständigkeit für IT-Sicherheit sowie Einvernehmensregelungen und Kooperation mit Regulierungsbehörden (Bundesnetzagentur), Landesbehörden und der Energiewirtschaft zur Entwicklung praxisnaher und durchsetzbarer Vorgaben.

d) Sensibilisierung und Ausbildung

- Schulung von Personal entlang der gesamten Wertschöpfungskette im Umgang mit Cybergefahren.
- Förderung von Fachkräften im Bereich IT-Sicherheit und OT-Sicherheit.

Das BSI stellt hierzu wertvolle Informationen auf Basis des festgestellten Lagebilds zur Verfügung.

e) Forschung und Innovation

- Unterstützung von Forschungsprojekten zur sicheren Integration erneuerbarer Energien durch BSI-Erkenntnisse und -Bewertungen.
- Integration wissenschaftlicher Erkenntnisse in die Entwicklung von Standards.
- Förderung der Entwicklung sicherheitsoptimierter Komponenten für Smart Grids und dezentrale Einspeiser.

7 Fazit

Der Energiesektor steht im Zentrum einer sicherheitsstrategischen Zeitenwende. Die zunehmende Digitalisierung, die Diversifizierung durch erneuerbare Energien und die angespannte geopolitische Lage erfordern ein Umdenken bei der Cybersicherheit. Deutschland muss proaktiv in Sicherheitsstrukturen, technische Schutzmaßnahmen und resiliente Architekturen investieren, um seine Energieversorgung langfristig zu sichern und die Risiken systemischer Ausfälle zu minimieren. Das BSI ist bereit mit seiner IT-Sicherheitsexpertise eine führende Rolle bei der Absicherung des Energiesektors zu übernehmen.