BSI

Positionspapier zu Cybersicherheit im Energiesektor

[22.05.2025] Das BSI warnt vor gravierenden Risiken für die Energieversorgung durch Cyberangriffe. In einem aktuellen Positionspapier fordert die Behörde umfassende Maßnahmen zur Stärkung der Cybersicherheit im Energiesektor.

Mit Blick auf die wachsenden Bedrohungen für Kritische Infrastrukturen warnt das Bundesamt für Sicherheit in der Informationstechnik (BSI) vor zunehmenden Gefahren für die Energieversorgung durch Cyberangriffe. In einem nun veröffentlichten Positionspapier skizziert die Behörde zentrale Herausforderungen sowie notwendige Maßnahmen für eine robuste Cybersicherheitsstrategie im Energiesektor.

Laut BSI steht die Energiebranche besonders im Fokus unterschiedlich motivierter Akteure: staatlich unterstützte Operationen verfolgen Ziele der Destabilisierung und Spionage, Cyberkriminelle setzen auf Erpressung, während so genannte Hacktivisten ideologische Interessen durch Angriffe auf Energieinfrastrukturen durchzusetzen versuchen. Der Handlungsbedarf sei dringend, so das BSI, das insbesondere auf die sich verschärfende geopolitische Lage und deren Einfluss auf die Motivationslage potenzieller Angreifer verweist.

„Eine erfolgreiche Störung der Energieversorgung in Deutschland oder Europa ist ein Schreckensszenario für Bürgerinnen und Bürger, die deutsche Wirtschaft und die staatlichen Organe“, erklärt BSI-Präsidentin Claudia Plattner. Die Auswirkungen eines solchen Szenarios wären laut Plattner gravierend: gesellschaftliches Leben käme zum Stillstand, wirtschaftliche Schäden wären immens. Investitionen in Sicherheitsstrukturen, technische Schutzmaßnahmen und resiliente Systemarchitekturen seien daher unumgänglich.

Das Positionspapier benennt zudem technische und strukturelle Entwicklungen, die die Bedrohungslage weiter verschärfen. Dazu zählen die zunehmende Dezentralisierung der Energieversorgung, die Digitalisierung von Netzen und Steuerungssystemen sowie die gestiegene Komplexität vernetzter Systeme. Weitere Risiken sieht das BSI in Angriffsmöglichkeiten entlang der Lieferkette, der Manipulation von Komponenten durch Hersteller oder Dritte sowie in bislang unbekannten Schwachstellen (Zero Days) industrieller Steuerungstechnik.

Als zentrale Maßnahme fordert das BSI sektorspezifische, einheitliche Sicherheitsanforderungen für alle Akteure – auch für kleinere Versorger, Netzbetreiber und Betreiber dezentraler Anlagen. Diese Standards sollen nicht unterhalb der sektorübergreifenden Mindestanforderungen liegen. Darüber hinaus plädiert das BSI für eine Stärkung aufsichtsrechtlicher Befugnisse und Interventionsmöglichkeiten bei Cybervorfällen. Die Behörde bietet an, mit ihrer Expertise eine koordinierende Rolle in der Cybersicherheit des Energiesektors zu übernehmen.

(th)

Stichwörter: Informationstechnik, Politik, Bundesamt für Sicherheit in der Informationstechnik (BSI), Cybersicherheit, Kritische Infrastrukturen (KRITIS)