Mitteilung

Power Systems

Kontakt Sebastian Steul
Telefon +49 69 66 03-1748
E-Mail sebastian.steul@vdma.org
Datum 16.10.2020

BSI-KritisV und IEC/ISO 27001 im Energieanlagenbau

Im Sinne des BSI zählen „Anlagen zur Erzeugung von elektrischer Energie“ sowie „Erzeugungsanlagen mit Wärmeauskopplung“ (KWK-Anlagen), „dezentrale Energieerzeugungsanlagen“ und „Speicheranlagen“ als kritische Infrastruktur, wenn sie den Durchschnitts-Jahresverbrauch von 500.000 versorgten Personen decken. Das entspricht einer Netto-Nennleistung von 420 MW (BSI-KritisV, Anhang 1, Teil 3, Nr.1.1.1 bis 1.1.5). Einschränkend zählt eine solche Anlage erst ab dem 01. April des Folgejahres als kritische Infrastruktur, nachdem sie den Schwellenwert von 420 MW das erste Mal erreicht hat. Dazu muss der Betreiber bis zum 31. März des Folgejahres die Leistung der Anlage im zurückliegenden Kalenderjahr ermitteln.

Kurzum: Alle Stromerzeugungsanlagen, die im Vorjahr eine Leistung von größer oder gleich 420 MW bereitgestellt haben, zählen nach BSI-KritisV als kritische Infrastruktur.

Dabei gilt auch, dass „Anlagen derselben Art [, die] in einem engen räumlichen und betrieblichen Zusammenhang“ stehen, als eine gemeinsame Anlage zählen. Ein enger räumlicher und betrieblicher Zusammenhang ist gegeben, „wenn die Anlagen

a) auf demselben Betriebsgelände liegen,
b) mit gemeinsamen Betriebseinrichtungen verbunden sind,
c) einem vergleichbaren technischen Zweck dienen und
d) unter gemeinsamer Leitung stehen.“ (BSI-KritisV, Anhang 1, Teil 1, Absatz 7).

Zudem gelten Heizkraftwerke als kritische Infrastruktur, wenn sie eine ausgeleitete Wärmeenergie von 2.300 GWh pro Jahr bereitstellen (BSI-KritisV, Anhang 1, Teil 3, Nr.4.1.2).

Virtuelle Kraftwerke oder standortübergreifende Steuerungen sind daher zum aktuellen Stand nicht durch die BSI-KritisV erfasst.

Nach Einschätzung des VDMA Power Systems hat die BSI-KritisV grundsätzlich keine direkten Auswirkungen auf die Hersteller von Energieanlagen, da sich die Verordnung ausschließlich auf die Betreiber von Energieanlagen bezieht

Anders verhält es sich mit den von Kundenseite vermehrt geforderten Zertifizierungsnachweisen. Konkret geht es in diesen Fällen um eine Zertifizierung nach

ISO/IEC 27001. Diese Norm wurde erarbeitet, um Anforderungen für die Einrichtung, Umsetzung, Aufrechterhaltung und fortlaufende Verbesserung eines Informationssicherheitsmanagementsystems (ISMS) festzulegen. Die Norm beschreibt somit den Prozess zur Einführung und zum Betrieb eines ISMS, nicht die technische Realisierung in einer Energieerzeugungsanlage. Bei der Forderung nach einer Zertifizierung handelt es sich grundsätzlich allerdings nicht um eine gesetzliche, sondern lediglich um eine vertragsrechtliche Anforderung, der Energieanlagenbauer nachkommen können, aber nicht müssen. Im Rahmen der „Supply Chain Security“ wird es aber zunehmend interessant für Betreiber, auf Komponenten und Anlagen zurückzugreifen, die nach Cybersecurity zertifiziert sind.

Welcher Bereich des Energieanlagenbau-Unternehmens letztlich zertifiziert wird, kommt aber vorrangig auf die individuellen Vertragsbedingungen an. VDMA Power Systems empfiehlt eine Zertifizierung nach ISO/IEC 27001 im Bereich der Fernwartung/ Steuerung von Energieanlagen. Darüber hinaus ist es sinnvoll, sich für die Produktsicherheit im Sinne der Cybersecurity mit der IEC 62443-4-1 und 62443-4-2 intensiv auseinanderzusetzen.

Für die IEC 62443 bietet der VDMA einen kostenfreien Leitfaden an, der angefordert werden kann.

Haben Sie noch Fragen? Wenden Sie sich gerne an Ihre Ansprechpartner im VDMA.

Ansprechpartner

Sebastian Steul
VDMA Power Systems
Referent Technologie & Innovation
Telefon: +49 69 6603-1748
E-Mail: sebastian.steul@vdma.org

Steffen Zimmermann
IT-Security, Industrial Security
Competence Center Industrial Security
Telefon: +49 69 6603-1978
E-Mail: steffen.zimmermann@vdma.org