TaylorWessing

Erneuerbare-Energien-Anlagen als Kritische Infrastruktur

Anforderungen an den IT-Schutz

Hintergrund

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) warnt bereits seit längerem vor erhöhten Gefahren für Erneuerbare-Energien-Anlagen (EE-Anlagen) und meldete konkrete Angriffe, darunter einen möglichen Cyberangriff auf tausende Windkraftanlagen im Februar 2022. Im April 2022 wurden die IT-Systeme der Deutsche Windtechnik, die für die Wartung von Windparks zuständig ist, angegriffen. Erst kürzlich kam es zu einem Cyberangriff auf die Deutsche Energie Agentur (DENA) sowie auf Enercity. Die Funktionsfähigkeit der Energieversorgung ist mehr denn je von einer intakten Informations- und Kommunikationstechnologie (IKT) abhängig.

Gesetzlich geregelt ist, wann Energieerzeugungsanlagen zur sogenannten Kritischen Infrastruktur gehören und damit besondere Anforderungen an den IT-Schutz erfüllen müssen. Im Sektor Energie (Stromversorgung) sind Kritische Infrastrukturen u.a. Erzeugungsanlagen, deren installierte Leistung bestimmte **Schwellenwerte** überschreitet. Mit der Absenkung der Schwellenwerte zum Januar 2022 gelten nun auch weniger große EE-Anlagen als Kritische Infrastruktur.

Mit unserem Guide „Erneuerbare-Energien-Anlagen als Kritische Infrastruktur – Anforderungen an den IT-Schutz“ greifen wir dieses zunehmend wichtige Thema auf und beantworten die wichtigsten energie- und IT-Schutz-rechtlichen Fragen.

EE-Anlagen als Kritische Infrastruktur: Die Gesetzeslage

Die Verpflichtungen für Betreiber Kritischer Infrastrukturen im Energiebereich sowie die Beantwortung der grundlegenden Frage, ob die betreffende Erzeugungsanlage als Kritische Infrastruktur einzuordnen ist, ergeben sich aus einer ganzen Reihe verschiedener Gesetze und Verordnungen:

- BSI-Gesetz (IT-Sicherheitsgesetz)
- BSI-KritisV
- EnWG
- T-Sicherheitskatalog der BNetzA

Im **BSIG** ist festgelegt, dass Kritische Infrastrukturen Einrichtungen, Anlagen oder Teile davon sind, die u.a. dem Sektor Energie angehören und die von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden (§ 2 Abs. 10). **Der BSI-KritisV** als auf dem BSIG basierende Verordnung kommt eine besondere Bedeutung zu. Hier wird anhand qualitativer und quantitativer Kriterien festgelegt, welche Infrastrukturen als kritisch gelten.

Im Sektor Energie (Stromversorgung) sind dies u.a. Erzeugungsanlagen sowie Anlagen oder Systeme zur Steuerung/Bündelung elektrischer Leistung. Ob eine Energieerzeugungsanlage als Kritische Infrastruktur gilt, hängt maßgeblich davon ab, ob die in Anhang 1 Teil 3 der KritisV festgelegten **Schwellenwerte** überschritten werden. Diese Schwellenwerte wurden zum Januar 2022 deutlich abgesenkt, wodurch auch weniger große EE-Anlagen in ihren Anwendungsbereich fallen. Galt bislang ein Schwellenwert von 420 MW, liegt der Schwellenwert für Erzeugungsanlagen nunmehr bei einer Nettonennleistung von lediglich 104 MW. Damit fallen viele Onshore Windparks, Solarparks und vor allem Offshore Windparks in den Anwendungsbereich der KritisV. Schwarzstartfähige Erzeugungsanlagen unterliegen unabhängig vom Umfang der installierten Leistung der KritisV. Bei Anlagen zur Erbringung von Primärregelleistung liegt der Schwellenwert bei 36 MW.

Schwellenwerte für Erzeugungsanlagen nach BSI-KritisV in MW

Installierte Nettonennleistung (elektrisch oder direkt mit Wärmeauskopplung verbundene elektrische Wirkleistung bei Wärmenennleistung ohne Kondensationsanteil)	Installierte Nettonennleistung, wenn die Anlage als Schwarzstartanlage nach § 3 Absatz 2 des Beschlusses der BNetzA vom 20. Mai 2020, Az. BK6-18-249 kontrahiert ist	Installierte Nettonennleistung, wenn die Anlage zur Erbringung von Primärregelleistung nach § 2 Nummer 8 StromNZV präqualifiziert ist
104 MW	0 MW	36 MW

Betreiber von EE-Anlagen

Betreiber ist nach § 1 Abs. 1 Nr. 2 KritisV eine natürliche oder juristische Person, die unter Berücksichtigung der rechtlichen, wirtschaftlichen und tatsächlichen Umstände **bestimmenden Einfluss** auf die Beschaffenheit und den Betrieb einer Anlage oder Teilen davon ausübt. Die Möglichkeit, bestimmenden Einfluss zu nehmen, hat, wer weisungsfrei und selbstständig über die Anlage oder Teile davon verfügen kann, wobei die rechtliche Verfügungsgewalt i. d. R. mit der tatsächlichen Sachherrschaft einhergeht. Bei der Beurteilung der wirtschaftlichen Umstände ist maßgebend, wer den wirtschaftlichen Nutzen aus der Anlage ziehen kann und wer das wirtschaftliche Risiko trägt. Die Betreibereigenschaft bestimmt sich nach einer **Gesamtbewertung** der vorgenannten Aspekte.

Es ist für die Betreibereigenschaft grundsätzlich unbeachtlich, wenn sich der Betreiber beim Betrieb der Anlage Dritter bedient, solange er den bestimmenden Einfluss über die Kritische Infrastruktur nicht zugleich selbst aufgibt. Auch wenn die tatsächliche Sachherrschaft bei einem beauftragten Dienstleister liegt, verbleibt durch vertraglich vermittelte Weisungs- und Kontrollrechte des Auftraggebers der bestimmende Einfluss i. d. R. weiterhin bei ihm. Etwas anderes kann jedoch gelten, wenn der Dienstleister seine Leistungen weitgehend weisungsunabhängig erbringt.

Eine Anlage kann nur einen verantwortlichen Betreiber haben (Grundsatz der **Betreiberidentität**). Hierdurch soll gewährleistet werden, dass Rechte und Pflichten klar zugewiesen werden können.

Anforderungen an die Informationssicherheit für Betreiber von EE-Anlagen, die als Kritische Infrastruktur gelten

Gemäß § 11 Abs. 1b EnWG sind Betreiber von Energieanlagen, die als Kritische Infrastruktur bestimmt wurden und an ein Energieversorgungsnetz angeschlossen sind, dazu verpflichtet, einen angemessenen Schutz gegen Bedrohungen für Telekommunikations- und elektronische Datenverarbeitungssysteme zu gewährleisten, die für einen sicheren Anlagenbetrieb notwendig sind. Ein angemessener Schutz liegt vor, wenn der **IT-Sicherheitskatalog gemäß § 11 Abs. 1b EnWG** der BNetzA eingehalten wird und dies vom Betreiber dokumentiert worden ist. Erforderlich ist demgemäß insbesondere die Implementierung eines **Informationssicherheits-Managementsystems (ISMS)**, das den Anforderungen der **DIN EN ISO/IEC 27001** entspricht. Bei der Implementierung des ISMS sind darüber hinaus die Normen **DIN EN ISO/IEC 27002 sowie 27019** in der jeweils gültigen Fassung zu berücksichtigen. Der Betreiber ist ferner verpflichtet, die Konformität seines ISMS durch ein Zertifikat einer für die Zertifizierung des IT-Sicherheitskatalogs bei der Deutschen Akkreditierungsstelle (DAkkS) akkreditierten unabhängigen Zertifizierungsstelle zu belegen. Die Einhaltung kann von der BNetzA überprüft werden. Spätestens ab dem am 1. Mai 2023 müssen Betreiber darüber hinaus angemessene Systeme zur Angriffserkennung einsetzen sowie dies dem BSI erstmalig an diesem Datum und danach alle zwei Jahre nachweisen, § 11 Abs. 1d, Abs. 1e EnWG.

Nachweise und Meldepflichten

Zunächst muss der Betreiber selbst die Einhaltung der Anforderungen des IT-Sicherheitskatalogs in Form eines Zertifikats nachweisen. Unabhängig davon muss auch der Betriebsführer bestimmte Sicherheitskriterien erfüllen, wobei der Nachweis durch ein eigenständiges Zertifizierungsverfahren erfolgt. Nähere Informationen sind in der **Mitteilung der BNetzA** zur Zertifizierung nach IT-Sicherheitskatalog § 11 Abs. 1a und 1b EnWG im Fall einer Betriebsführung durch Dritte zu finden.

Gemäß § 11 Abs. 1c EnWG haben Betreiber von Energieanlagen, die als Kritische Infrastruktur bestimmt wurden, Störungen, die zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Funktionsfähigkeit der betreffenden Energieanlage geführt haben, oder erhebliche Störungen, die zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Funktionsfähigkeit der betreffenden Energieanlage führen können, **unverzüglich** – also ohne schuldhaftes Zögern – über die Kontaktstelle an das BSI zu melden. Eine Störung liegt vor, wenn die eingesetzte Technik die ihr zugedachte Funktion nicht mehr richtig oder nicht mehr vollständig erfüllen kann oder versucht wurde, entsprechend auf sie einzuwirken.

Registrierungs- und sonstige Pflichten

Betreiber Kritischer Infrastrukturen sind verpflichtet, die von ihnen betriebenen Anlagen beim BSI zu registrieren und eine Kontaktstelle zu benennen, § 8b Abs. 3 BSIG. Darüber hinaus ist sicherzustellen, dass der Betreiber über die Kontaktstelle jederzeit erreichbar ist. Die Registrierung hat spätestens bis zum ersten Werktag, der darauf folgt, dass die Anlage erstmalig oder erneut als Kritische Infrastruktur gilt, zu erfolgen.

Grundsätzlich haben Betreiber Kritischer Infrastrukturen den geplanten erstmaligen Einsatz einer sog. kritischen Komponente (§ 2 Abs. 13 BSIG) dem BMI vor ihrem Einsatz anzuzeigen, § 9b Abs. 1 BSIG. Kritische Komponenten sind nur solche, die konkret per Gesetz definiert werden. Bisher ist diese Anzeigepflicht vor allem im Bereich Telekommunikation relevant.

Bußgelder bei Nichteinhaltung der vorgenannten Pflichten

Grundsätzlich können Verstöße gegen das BSIG mit Geldbußen i. H. v. bis zu 20 Mio. Euro geahndet werden; das EnWG sieht einen Bußgeldrahmen von bis zu 5 Mio. Euro vor. Aufgrund der abgestuften Sanktionskataloge sind diese Beträge jedoch nur bei bestimmten – besonders schwerwiegenden – Verstößen einschlägig, wie beispielsweise bei Zuwiderhandlungen gegen bestimmte vollziehbare Anordnungen des BSI.

Demgegenüber stellen Verstöße gegen die IT-Sicherheits- und Meldepflichten des § 11 EnWG gemäß § 95 Abs. 1 Nr. 2a, 2b EnWG Ordnungswidrigkeiten dar, die mit einer Geldbuße i. H. v. bis zu hunderttausend Euro geahndet werden können, § 95 Abs. 2 Satz 1 EnWG. Ein Verstoß gegen die Registrierungspflicht aus § 8b Abs. 3 BSIG ist gemäß § 14 Abs. 2 Nr. 5, Abs. 5 Satz 2 BSIG mit einer Geldbuße i. H. v. bis zu fünfhunderttausend Euro bedroht; die fehlende Sicherstellung der Erreichbarkeit der Kontaktstelle mit einer Geldbuße i. H. v. bis zu einhunderttausend Euro, § 14 Abs. 2 Nr. 6, Abs. 5 Satz 2 BSIG.

TaylorWessing

Ausblick

Grundsätzlich sind Änderungen der bestehenden gesetzlichen Rahmenbedingungen zu erwarten, denn auf europäischer Ebene ist die NIS2-Richtlinie, eine EU-weite Gesetzgebung zur Netzwerk- und Informationssicherheit, am 16. Januar 2023 in Kraft getreten. Die Mitgliedstaaten müssen die Richtlinie bis zum 17. Oktober 2024 in nationales Recht umsetzen.

In Deutschland gibt es bereits einen Referentenentwurf des Bundesinnenministeriums zur Umsetzung der NIS-2-Richtlinie (NIS-2UmsuCG). Durch die NIS2-Richtlinie sollen die Anforderungen an die Cybersicherheit erhöht und mitgliedstaatliche Anforderungen vereinheitlicht werden. Insbesondere soll es keine sektorspezifischen Schwellenwerte mehr geben, sondern in erster Linie das Tätigkeitsfeld eines Unternehmens sowie dessen Größe (Mitarbeiteranzahl sowie Jahresumsatz bzw. -bilanz) wird entscheiden, ob es als „wesentliche" oder „wichtige Einrichtung" dem Anwendungsbereich der Richtlinie unterfällt. Auf der Rechtsfolgenseite sollen die Anforderungen an ein hinreichendes Cybersicherheitsrisikomanagement erhöht sowie die Meldepflichten ausgedehnt werden. Ferner werden den Behörden erweiterte Befugnisse zugestanden. Angesichts drohender Bußgelder in Höhe von bis zu 10 Mio. EUR oder bis zu 2 % des gesamten weltweiten im vorangegangenen Geschäftsjahr getätigten Umsatzes sollten Unternehmen die weiteren Entwicklungen wachsam verfolgen, um rechtzeitig die zur NIS-2-Compliance erforderlichen Schritte einleiten zu können.

Ihre Ansprechpartner

Dr. Paul Voigt, Lic. en Derecho, CIPP/E
Berlin
+49 30 885636-408
p.voigt@taylorwessing.com

Dr. Markus Böhme, LL.M. (Nottingham)
Düsseldorf
+49 211 8387-430
m.boehme@taylorwessing.com