IT-Sicherheit von Windenergieanlagen

18.01.2019 – Energierecht, Erneuerbare-Energien-Recht, IT- und Onlinerecht, Verwaltungsrecht, Windenergie, Newsletter

Unsere moderne Gesellschaft ist in hohem Maße von einer funktionierenden Energieversorgung abhängig. Fehlen Strom und Gas, kommt das öffentliche Leben innerhalb kürzester Zeit zum Erliegen und lebensnotwendige Dienstleistungen können nicht mehr erbracht werden. Gleichzeitig ist die Funktionsfähigkeit der Energieversorgung von einer intakten Informations- und Kommunikationstechnologie (IKT) abhängig. Jedoch seien einige Windkraftanlagen und Windparks nach Ansicht von Experten nicht ausreichend geschützt, wenn sie ins Visier von Hackern geraten. Es drängt sich daher zunehmend die Frage auf, inwiefern der Gesetzgeber den Betreibern von Windenergieanlagen Sicherheitspflichten auferlegt, oder ob eine defizitäre Ausgestaltung zur Achillesverse des Energiesektors wird.

Im Juli 2015 trat das Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) für Betreiber sog. Kritische Infrastrukturen in Kraft. Das Gesetz erweitert die bestehenden Regelungen zur IT-Sicherheit im „Gesetz über das Bundesamt für Sicherheit in der Informationstechnik“ (BSIG) und im Energiewirtschaftsgesetz (EnWG). Ziel dieses Gesetzes ist es, die Sicherheit informationstechnischer Systeme von Kritischen Infrastrukturen zu verbessern und Zugriffe von außen zu verhindern. Die am 3. Mai 2016 in Kraft getretene Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSIG (BSI-KritisV) bestimmt qualitative und quantitative Kriterien, anhand derer Betreiber nunmehr feststellen können, ob die von ihnen betriebene Anlage als Kritische Infrastrukturen einzustufen sind.

Als Betreiber Kritischer Infrastrukturen gelten zum einen, die Betreiber von (dezentralen) von Erzeugungsanlagen mit einer installierten Netto-Nennleistung von 420 MW (insbesondere große Offshore-Windparks), zum anderen Betreiber von Anlagen und Systemen zur Steuerung oder Bündelung elektrische Leistung (Aggregatoren/Virtuelle Kraftwerke), mit denen auf (dezentrale) Erzeugungsanlagen oder Verbrauchereinrichtungen mit einer kumulierten installierten Leistung von insgesamt mindestens 420 MW zugegriffen wird.

Die Pflichten zur Umsetzung von IT-Sicherheitsanforderung ergeben sich jedoch nicht unmittelbar aus dem IT-Sicherheitsgesetz oder aus der BSI-KritisV. Umsetzungspflichten ergeben sich zunächst für sämtliche Unternehmen, d.h. auch für Betreiber nicht-kritischer Infrastrukturen (< 420 MW), aus allgemeinen Sorgfaltspflichten, denen insbesondere die Unternehmensleitung unterliegt (z.B. gem. AktG und GmbHG). Hinzu kommen für Betreiber Kritischer Infrastrukturen zusätzliche Umsetzungsanforderung aus den jeweiligen Spezialgesetzen (u.a. dem EnWG und dem BSIG). Gem. § 11 Abs. 1b EnWG sind Betreiber von Erzeugungsanlagen verpflichtet, einen „angemessenen Schutz“ gegen Bedrohungen für Telekommunikations- und elektronische Datenverarbeitungssysteme zu gewährleisten, die für einen sicheren Anlagebetrieb notwendig sind. Was unter „angemessenen Schutz“ zu verstehen ist, richtet sich gem. § 11 Abs. 1b S.2 EnWG nach einem Katalog von

martin@maslaton.de http://www.maslaton.de

Sicherheitsanforderungen (IT-Sicherheitskatalog), der von der Bundesnetzagentur im Benehmen mit dem BSI erstellt wird.

Der Katalog bezieht sich aktuell nur auf Energieerzeugungsanlagen im engeren Sinne. Nach Auffassung des BSI und BNetzA sind vom Begriff „Energieanlagen“ nur noch solche erfasst, die der Erzeugung oder Verteilung von Energie dienen, nicht jedoch Anlagen und Systeme zur reinen Signalübertragung. Die Anlagen und Systeme etwa von Direktvermarktern dienen eben nicht der Stromerzeugung wie die Windenergieanlagen selbst. Es handelt sich grundsätzlich um separat zu betrachtende Systeme. Sie sind daher vom Katalog nicht betroffen.

Ferner setzt dieser Sicherheitskatalog zur Erreichung der Schutzziele auf einen ganzheitlichen Ansatz, der kontinuierlich auf Leistungsfähigkeit und Wirksamkeit zu überprüfen und bei Bedarf anzupassen ist. Einen solchen ganzheitlichen Ansatz stellt ein sog. Informationssicherheits- Managementsystem (ISMS) dar. Auch im Bereich nicht-kritischer Infrastrukturen (<420 MW) gelten Mindestanforderung, die Unternehmen im Bereich der IT-Sicherheit zu ergreifen haben. Diese sind im Gesellschaftsrecht verankert. Gem. § 93 Abs.1 AktG und § 43 GmbHG hat die Geschäftsleitung eines Unternehmen in der Betriebsorganisation die Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiter zu beachten. Dies umfasst auch Maßnahmen im Bereich der IT-Sicherheit. Der Umfang ist jeweils abhängig vom konkreten Geschäftsbetrieb und Risikoprofil eines Unternehmens. Als Indikator für angemessene IT-Sicherheitsmaßnahmen können u.a. die Errichtung eines Früherkennungssystems, die Einrichtung eines Risikomanagement- und Reporting-Systems, die Zuordnung von IT-Verantwortung in der Unternehmensorganisation, als auch die Beachtung technischer Regelwerke, dienen.

Fazit: Schließlich lässt sich somit festhalten, dass der IT-Sicherheit ausreichend Rechnung getragen wird. Insbesondere durch die hohen Anforderungen des „IT-Sicherheitskatalogs“, als auch durch das Ermöglichen einer persönlichen Haftung von Geschäftsführer und Vorstand, in Folge der sog. „Business Judgment Rule“ (§ 93 Abs. 1 AktG; § 43 GmbHG), kann daher die geäußerte Kritik insoweit entschärft werden. Jedoch ist es stets erforderlich, die Sicherheitsmaßnahmen permanent auf einem hohen Niveau zu halten, um mit dem rasanten Tempo der technischen Entwicklung Schritt zu halten und den Anschluss nicht zu verlieren.

martin@maslaton.de
http://www.maslaton.de