Quelle: A.Zerndl/123RF.com

Novellierte BSI-Kritisverordnung

Schwellenwerte für Energieerzeugungsanlagen gesunken

Am 1. Januar 2022 ist die Novelle der Verordnung zur Bestimmung kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-KritisV) in Kraft getreten. Die Verordnung regelt, welche Betreiber kritischer Infrastrukturen besondere IT-Sicherheitsstandards erfüllen müssen. Auch die Energiewirtschaft zählt zu den sicherheitsrelevanten Sektoren und ist von den Änderungen betroffen: Mit der Novelle sinken unter anderem die Schwellenwerte für Erzeugungsanlagen. Dadurch können auch weniger große Anlagen in den Anwendungsbereich der Regelung fallen – zum Beispiel Gaskraftwerke und Windparks.

Der Energiesektor und damit auch die Branche der erneuerbaren Energien sehen sich – wie viele weitere Bereiche der Industrie – zunehmend Cyberangriffen ausgesetzt. Der Gesetzgeber hat diese Gefahr erkannt und begegnet ihr in unterschiedlichen Gesetzen und Vorschriften. Das Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz) enthält wesentliche Vorschriften. Es normiert den rechtlichen Rahmen für das Bundesamt für Sicherheit in der Informationstechnik (BSI) als Bundesoberbehörde und die Betreiber von Anlagen, die als kritische Infrastruktur zu qualifizieren sind (Kritis-Anlagen). Ferner ist für den Sektor der Erneuerbare-Energien-Anlagen § 11 Energiewirtschaftsgesetz (EnWG) von erheblicher Bedeutung.

Was genau unter den Begriff der Kritis-Anlagen zu verstehen ist, ergibt sich aus der BSI-KritisV. Diese definiert die Sektoren, die aufgrund ihrer Bedeutung Anlagen aufweisen, die als kritische Infrastruktur zu qualifizieren sind (Kritis-Anlagen). Für jeden dieser Sektoren bestimmt die BSI-KritisV Anlagenkategorien und Schwellenwerte, bei deren Annahme eine Kritis-Anlage zu bejahen

ist. Der Energiesektor gehört zu diesen relevanten Sektoren. Eine der hierunter aufgeführten Anlagenkategorien ist die der Erzeugungsanlagen.

Des Weiteren erfasst die BSI-KritisV die Kategorie der »Anlagen oder Systeme zur Steuerung/Bündelung elektrischer Leistung«. Software beziehungsweise IT-Systeme von Betriebsführern oder Wartungsunternehmen (Stichwort: Leitwarte), Umspannwerke sowie virtuelle Kraftwerke können hierunter fallen, sofern durch diese eine den Schwellenwert übersteigende elektrische Leistung kontrolliert wird. Um als Kritis-Anlage zu gelten, müssen Software beziehungsweise IT-Systeme aber eine tatsächlich steuernde Einflussnahme zum Beispiel auf elektrische Leistung produzierende Anlagen ermöglichen.

Stark gesenkte Schwellenwerte: Mehr Betreiber von Energieerzeugungsanlagen betroffen

Die neue Fassung der BSI-KritisV sieht erhebliche Änderungen vor. Seit diesem Jahr gilt ein deutlich niedrigerer Schwellenwert: Er sinkt von 420 MW auf 104 MW installierte Nettonennleistung. Unabhängig vom Schwellenwert unterliegen Erzeugungsanlagen stets der BSI-KritisV, wenn sie als Schwarzstartanlagen vereinbart sind. Dienen sie der Erbringung von Primärregelleistung, liegt der Schwellenwert bei 36 MW.

Durch die Änderungen der BSI-KritisV werden geschätzt 252 neue Betreiber erfasst, wovon 130 Betreiber dem Bereich der Stromerzeugung zuzuordnen sind. Möglicherweise hiervon Betroffene sollten also möglichst schnell die eigene Betreiberrolle überprüfen. Dies ist Pflicht eines jeden Betreibers selbst.

Welche Pflichten haben die Betreiber von Kritis-Anlagen?

Grundlegend lassen sich die mit einer Einordnung als Kritis-Anlage verbundenen Pflichten in die nachfolgenden zwei Kategorien einteilen:

1. IT-Sicherheitsstandards
2. Registrierungs-/Nachweis-/Meldepflichten.

Betreiber von Kritis-Anlagen müssen einen bestimmten IT-Sicherheitsstandard einführen – mit Zertifizierung beziehungsweise Einzelnachweis – sowie die Aufrechterhaltung sicherstellen und alle zwei Jahre nachweisen. Gegenstand dieses Standards ist grundsätzlich ein Informationssicherheits-Managementsystem (ISMS) gemäß DIN EN ISO/IEC 27001. Die spezifische Ausgestaltung des IT-sicherheitstechnischen Mindeststandards hängt von der Kategorie der Kritis-Anlage ab. Für die Betreiber von Windenergieanlagen ist der in Zusammenarbeit zwischen dem BSI und der Bundesnetzagentur erstellte IT-Sicherheitskatalog maßgeblich (vgl. § 11 Abs. 1b EnWG). Sofern zum Beispiel Betriebsführer oder Wartungsunternehmen Kritis-Anlagen betreiben, wird der branchenspezifische Sicherheitsstandard durch den Bundesverband der Energie- und Wasserwirtschaft e. V. vorgegeben (vgl. § 8a Abs. 2 S. 1 BSI-Gesetz).

Darüber hinaus haben alle Betreiber von Kritis-Anlagen diese beim BSI zu registrieren. Dabei ist auf Seiten des Betreibers auch eine Kontaktstelle zu benennen, die jederzeit erreichbar sein muss. Ferner treffen die Betreiber Meldepflichten gegenüber dem BSI im Fall von (erheblichen) Störungen ihrer IT-Systeme. Die konkrete Ausgestaltung der Meldepflicht variiert je nach Art der Störung und Schadensumfang. Verstöße gegen Vorschriften des BSI-Gesetzes können zum Beispiel behördliche Aufsichts- und Informationsmaßnahmen, Bußgelder bis zu 2 Mio. € sowie die zivilrechtliche Haftung gegenüber Dritten zur Konsequenz haben.

IT-Sicherheit für nicht-kritische Infrastruktur

Allerdings unterliegen auch die Betreiber nicht-kritischer Infrastruktur Pflichten zur IT-Sicherheit – wenn auch nur in abgeschwächtem Umfang. Die Rechtsquellen hierfür variieren und ebenso das Maß an Verbindlichkeit. Wesentlich ist aber die »Sorgfaltspflicht der Geschäftsleitung«, aus der mitunter zivilrechtliche Haftungsansprüche resultieren können. Demnach hat die Geschäftsführung geeignete Maßnahmen zu treffen, um einen hinreichenden IT-Sicherheitsstandard zu gewährleisten. Denkbare Maßnahmen sind zum Beispiel ein Risikomanagement- und Reporting-System, der Aufbau von IT-Know-how verbunden mit klarem Verantwortungsbereich, Schulungen, Vor-Ort-Maßnahmen oder die Umsetzung technischer Regelwerke.

Ungeachtet dessen sollten IT-Sicherheitsmaßnahmen bereits aus wirtschaftlichem Eigeninteresse eingeführt und regelmäßig überprüft werden. Cyberattacken konzentrieren sich zunehmend weniger auf große Unternehmen. Vielmehr sind immer mehr Unternehmen zufällig im Rahmen von Ransomware-Angriffen betroffen. Diese bewirken einen Kontrollverlust über die betroffenen IT-Systeme und gehen oft mit der Forderung zur Zahlung von Lösegeld zwecks Systemfreigabe einher.

Fazit

Mit einer zunehmenden Dezentralisierung der Energieerzeugungsstruktur und der Stilllegung großer Kraftwerke nimmt die systemische Relevanz auch kleinerer Anlagen wie Windparks zu. Eine Anpassung der Schwellenwerte für Energieerzeugungsanlagen und vor allem für Software zur Steuerung dieser ist daher sinnvoll. Die betroffenen Betreiber müssen sich nun konkret mit der Ausgestaltung der für sie erforderlichen IT-Sicherheit auseinandersetzen.

David Ferrazini,
Rechtsanwalt,
Sterr-Kölln & Partner, Freiburg

>> david.ferrazini@sterr-koelln.com
>> www.sterr-koelln.com