IM FOKUS

Unter Strom: Auswirkungen des IT-Sicherheitsgesetzes im Energiesektor

Die fortschreitende Digitalisierung ist auch für Energieversorgungsunternehmen (EVU) ein wichtiges Thema. Operative Prozesse wie Netzbetrieb, -management und -stabilisierung erfahren zunehmend einen fundamentalen Wandel: die Verzahnung einst strikt voneinander getrennter IT-Welten. Dies birgt jedoch zwangsläufig neue Gefahren für die Informationstechnik. Hier treten das IT-Sicherheitsgesetz und der IT-Sicherheitskatalog auf den Plan – und setzen EVU vor allem durch die damit verbundenen Fristen unter Strom.

Informationstechnik nimmt immer stärkeren Einfluss auf die Effizienz und Wirtschaftlichkeit von Energieversorgern. Effizienzgewinne basieren hier meist auf der Öffnung der bislang getrennten Welten von kaufmännischer IT und operativer Anlagensteuerung. Ein Beispiel dafür ist Smart Grid: Um die Erzeugung, Verteilung und Speicherung von Energie intelligent zu koordinieren, müssen Steuerungs- und Betriebsinformationen zwischen Strom- und Datennetzen ausgetauscht werden. Als Datenschnittstelle zwischen privatem Haushalt, Netzbetreiber und Energielieferant dienen Smart Meter. In Netzkontrollzentren laufen alle relevanten Informationen wie Spannungsschwankungen, Verbrauchsdaten und Fehlermeldungen zusammen. So ermöglicht die digitale Kommunikation aller Beteiligten, die Energiezufuhr sämtlicher dezentraler Quellen bedarfsgerecht zu steuern.

Nicht immer gehen diese Entwicklungen mit einem steigenden Sicherheitsniveau einher. Umfragen zeigen, dass bei der Absicherung von Informationsinfrastrukturen klarer Nachholbedarf besteht.[1] Vor dem Hintergrund, dass die IT-Systeme der EVU durch die fortschreitende Digitalisierung maßgeblich die Versorgungssicherheit der Bevölkerung beeinflussen, ist diese Entwicklung insbesondere im Energiesektor bedenklich.

Der Gesetzgeber hat daher die Notwendigkeit einer Regulierung gesehen. Seit 25. Juli 2015 in Kraft, macht das IT-Sicherheitsgesetz explizite Vorgaben für die Sicherheit informationstechnischer Systeme. Es zielt darauf ab, elementare Versorgungsinfrastrukturen wie Kraftwerke, Mobilfunknetze oder Krankenhäuser in ihrer Funktionsfähigkeit abzusichern und ein hinreichendes Schutzniveau zu erreichen.[2] Im Energiesektor existiert neben dem IT-Sicherheitsgesetz eine weitere Vorgabe: Auf Basis des Energiewirtschaftsgesetzes (EnWG) hat die Bundesnetzagentur (BNetzA) im August 2015 den „IT-Sicherheitskatalog gemäß § 11 Absatz 1a Energiewirtschaftsgesetz" erlassen, der für Energienetzbetreiber spezifizierte Anforderungen an die IT-Sicherheit nennt und ergänzend zum IT-Sicherheitsgesetz zu sehen ist.

Die Fristen für die Umsetzung der regulatorischen Anforderungen sind eng bemessen. Der letzte Termin für die Umsetzung des IT-Sicherheitsgesetzes ist der 2. Mai 2018[3], für den IT-Sicherheitskatalog sogar schon der 31. Januar 2018. Energieversorger sind daher unter Zugzwang und müssen aktiv werden. Fallen sie unter das IT-Sicherheitsgesetz, den IT-Sicherheitskatalog oder gegebenfalls unter beides? Welche Anforderungen müssen sie erfüllen? Welche Hindernisse gilt es zu nehmen?

Geltungsbereich des IT-Sicherheitsgesetzes

Da der Geltungsbereich des IT-Sicherheitsgesetzes im Gesetz selbst nur unspezifisch beschrieben wird, hat das Bundesinnenministerium am 3. Mai 2016 die erste Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-KritisV) erlassen. Diese regelt unter anderem den Geltungsbereich für den Energiesektor.

1 Vgl. KPMG International (2015): Cyber security: A failure of imagination by CEOs, S. 4; KPMG International (2016): Now or never: 2016 Global CEO Outlook, S. 29; Bundesamt für Sicherheit in der Informationstechnik (2015): Die Lage der IT-Sicherheit in Deutschland 2015, S. 42

2 Vgl. auch: Dolle, W. / Redlich, T. / Tiedemann, J.: Das IT-Sicherheitsgesetz – lästig oder längst überfällig? In: PublicGovernance Winter 2014

3 Das IT-Sicherheitsgesetz nennt eine Umsetzungsfrist von zwei Jahren nach Inkrafttreten der zugehörigen Verordnung.

© 2016 Institut für den öffentlichen Sektor e.V. Alle Rechte vorbehalten.

Die Verordnung zielt auf Betreiber ab, deren Anlagen[4] die Versorgungssicherheit von mindestens 500.000 Personen beeinflussen können. Um zu ermitteln, ob eine Anlage eine kritische Infrastruktur (KRITIS) ist, hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) kritische Versorgungsdienstleistungen wie „Stromversorgung" und Anlagenkategorien wie „Erzeugungsanlage" oder „Übertragungsnetz" definiert. Zugeordnete Schwellenwerte kombiniert mit einem Bemessungskriterium legen fest, ob ein Unternehmen oder Unternehmensteile vom Gesetz betroffen sind. Für Energieerzeugungsanlagen dient etwa die „installierte Netto-Nennleistung (elektrisch) in Megawatt" als Bemessungskriterium, wobei der Schwellenwert bei 420 MW liegt. Hintergrund: Bei einem jährlichen Durchschnittsverbrauch von 7.375 kWh pro Kopf werden 420 MW Nennleistung benötigt, um den Energiebedarf von 500.000 Personen zu decken.

Unternehmen sind grundsätzlich selbst dafür verantwortlich zu evaluieren, ob sie als KRITIS-Betreiber gelten. Dabei muss ein EVU zunächst feststellen, ob es eine der definierten kritischen Versorgungsdienstleistungen erbringt und welche Anlagen hierfür notwendig sind. In einem zweiten Schritt muss bestimmt werden, ob die Anlagen anhand der festgelegten Schwellenwerte als kritisch gelten.

Diese Evaluation muss jährlich bis zum 31. März auf Basis der Daten des zurückliegenden Kalenderjahres erfolgen.[5] Ein EVU muss somit jedes Jahr erneut bewerten, ob es eine kritische Infrastruktur betreibt. Erreicht oder überschreitet eine Anlage den in der BSI-Kritisverordnung angegebenen Versorgungsgrad, so gilt sie zum 1. April als kritische Infrastruktur.

Anforderungen des IT-Sicherheitsgesetzes

Das IT-Sicherheitsgesetz gibt drei verpflichtende zentrale Anforderungen für KRITIS-Betreiber vor.[6] Für betroffene Energieversorger heißt das:

1. **Meldepflicht:** EVU müssen dem BSI Warn- und Alarmierungskontakte nennen. Vorfälle, welche die IT-Sicherheit tangieren und die Aufrechterhaltung kritischer Versorgungsdienstleistungen bedrohen können, müssen umgehend an das BSI gemeldet werden. Das betrifft etwa das Auffinden unerwarteter Schadprogramme wie im April 2016 im Atomkraftwerk Gundremmingen.[7]

2. **Sicherheitsmaßnahmen:** EVU müssen umfangreiche technische und organisatorische Maßnahmen ergreifen, über die sich das gesetzliche Mindestmaß an IT-Sicherheit definiert. Allgemeine Vorkehrungen, zum Beispiel die Einrichtung eines Notfallmanagementprozesses, sind um branchenspezifische Sicherheitsmaßnahmen wie die Erstellung eines Netzstrukturplans gemäß IT-Sicherheitskatalog zu erweitern.

3. **Nachweis:** Mindestens alle zwei Jahre haben EVU gegenüber dem BSI zu belegen, dass sie den Vorgaben des IT-Sicherheitsgesetzes in Bezug auf orga-

4 Anlagen sind Betriebsstätten oder sonstige ortsfeste Einrichtungen sowie Maschinen, Geräte und sonstige ortsveränderliche Einrichtungen, die für die Dienstleistungserbringung notwendig sind.

5 Erfolgt die Ermittlung anstelle von Schwellenwerten unmittelbar anhand der Anzahl angeschlossener Haushalte, ist der Versorgungsgrad zum 30. Juni des zurückliegenden Kalenderjahres maßgeblich. Diese Regelung betrifft im Energiesektor jedoch ausschließlich die Anlage „Fernwärmenetz".

6 Bereits in der Entwurfsphase des IT-Sicherheitsgesetzes hat KPMG die Anforderungen für KRITIS-Betreiber ausführlich erläutert (siehe „Das IT-Sicherheitsgesetz – lästig oder längst überfällig?", PublicGovernance Winter 2014).

7 Vgl. Zeit Online (2016): Computervirus in bayerischem Atomkraftwerk entdeckt, www.zeit.de/digital/2016-04/gundremmingen-atomkraftwerk-computervirus, 26.4.2016

© 2016 Institut für den öffentlichen Sektor e.V. Alle Rechte vorbehalten.

nisatorische und technische Maßnahmen sowie hinsichtlich der Meldepflicht nachkommen.

Geltungsbereich und Anforderungen des IT-Sicherheitskatalogs

Der IT-Sicherheitskatalog regelt die Umsetzungsverpflichtung zur Absicherung jener IT- und datenverarbeitenden Systeme, die für einen sicheren Energienetzbetrieb notwendig sind. Er betrifft somit alle Betreiber von Elektrizitäts- und Gasversorgungsnetzen.[8]

Das EnWG bestimmt, dass mit Umsetzung des IT-Sicherheitskatalogs „ein angemessener Schutz des Betriebs eines Energieversorgungsnetzes" vorliegt. Hierfür werden drei Anforderungen genannt:

1. **Ansprechpartner:** Bis zum 30. November 2015 mussten Netzbetreiber der BNetzA einen Ansprechpartner für IT-Sicherheit benennen.

2. **Netzstrukturplan:** Netzbetreiber müssen einen Netzstrukturplan erstellen – eine Übersicht über alle Anwendungen, Systeme und Komponenten, die für einen sicheren Netzbetrieb notwendig sind. Dies umfasst auch die anzutreffenden Haupttechnologien sowie deren Verbindungen.

3a. **Informationssicherheitsmanagementsystem:** Die Kernforderung des IT-Sicherheitskatalogs liegt in der wirksamen Einführung eines Informationssicherheitsmanagementsytems (ISMS) nach DIN ISO/IEC 27001.[9] Das ISMS ist eine virtuelle Organisationseinheit, das Prozesse, Rolle, Verantwortlichkeiten und Ressourcen umfasst. Es bildet so einen Steuerungsrahmen für die zahlreichen auf Informationssicherheit ausgerichteten Aktivitäten und legt fest, wie sie nachvollziehbar koordiniert werden.

3b. **Zertifizierung des ISMS:** Über die Implementierung hinaus fordert der IT-Sicherheitskatalog eine anerkannte Zertifizierung des ISMS; hierzu erarbeitet die BNetzA gemeinsam mit der Deutschen Akkreditierungsstelle (DAkkS) ein Zertifizierungsschema auf Basis von DIN ISO/IEC 27001. Die Zertifizierung muss bis zum 31. Januar 2018 durch eine akkreditierte Zertifizierungsstelle abgeschlossen sein.

Abbildung 1: Navigationshilfe im Energiesektor

Quelle: KPMG AG Wirtschaftsprüfungsgesellschaft, 2016

Aus der verpflichtenden Anwendungdes DIN ISO / IEC 27001 ergibt sich für Energieversorger die Notwendigkeit zur Umsetzung einzelner Sicherheitsmaßnahmen. Dabei müssen alle im Anhang (Annex A) des Standards genannten Bereiche, zum Beispiel physische Sicherheit, betrachtet werden. In jedem Bereich fordert der Standard gewisse Sicherheitsmaßnahmen, etwa Zutrittskontrollen oder die Einrichtung von Sicherheitszonen. Zur Umsetzung der Maßnahmen kann auf die Best Practices der DIN ISO/IEC 27002[10] zurückgegriffen werden.

Netzbetreiber müssen darüber hinaus die Empfehlungen der DIN ISO/IEC TR 27019[11] umsetzen, die energiespezifische Maßnahmen nennt, zum Beispiel für die logische Anbindung von externen Prozesssteuerungssystemen. Das neue Zertifizierungsschema der BNetzA für Energieversorger wird daher nicht nur die Erfüllung des ISO/IEC 27001, sondern auch der DIN ISO/IEC 27019 betrachten.

Was gilt es zu tun? Herausforderungen und Lösungsansätze

Betroffenheitsanalyse: Ein EVU sollte zunächst klären, ob es durch das IT-Sicherheitsgesetz oder den IT-Sicherheitskatalog betroffen ist. Dies bedingt sich weder gegenseitig noch schließt es sich aus. Kleinere Stadtwerke gelten etwa anhand der Schwellenwerte meist nicht als KRITIS, müssen aber unabhängig von ihrer Größe die Vorgaben des IT-Sicherheitskatalogs erfüllen, wenn sie ein Energienetz betreiben (siehe Abbildung 1).

Ist ein EVU durch eine oder beide gesetzlichen Vorgaben betroffen, gilt es zu berücksichtigen, dass die geforderten Sicherheitsmaßnahmen nicht per se auf das gesamte Unternehmen angewendet werden müssen. Geschützt werden müssen nur jene Anlagen und Prozesse, die zur Erbringung einer kritischen Ver-

8 Ein zweiter IT-Sicherheitskatalog nach § 11 Abs. 1b EnWG wird ab dem vierten Quartal 2016 erwartet. Er betrifft Betreiber von Energieanlagen mit Anschluss an ein Energieversorgungsnetz, die anhand der BSI-KritisV als KRITIS-Betreiber gelten.

9 Die Forderung nach einem ISMS ist auch im IT-Sicherheitsgesetz enthalten, wird dort aber implizit über Sicherheitsmaßnahmen nach dem Stand der Technik definiert. Der IT-Sicherheitskatalog fordert das ISMS ausdrücklich.

10 Titel: „Informationstechnik – IT-Sicherheitsverfahren – Leitfaden für das Informationssicherheits-Management"

11 Titel: „Informationstechnik – Sicherheitsverfahren – Leitfaden für das Informationssicherheitsmanagement von Steuerungssystemen der Energieversorgung auf Grundlage der ISO/IEC 27002"

© 2016 Institut für den öffentlichen Sektor e.V. Alle Rechte vorbehalten.

sorgungsdienstleistung notwendig sind. Daher kann das ISMS auf einzelne Unternehmensbereiche, Prozesse oder Abteilungen beschränkt werden. Voraussetzung hierfür sind eine Analyse der Unternehmensprozesse sowie eine Bestandsaufnahme der Werte und Anlagen, um notwendige Ressourcen für die kritischen Versorgungsdienstleistungen und Abhängigkeiten zwischen Prozessen aufzudecken. Die erfassten Werte und Anlagen können direkt in die Kategorien „Leitsysteme und Systembetrieb", „Übertragungstechnik/Kommunikation" und „Sekundär-, Automatisierungs- und Fernwirktechnik" eingeordnet werden. Dies erleichtert die Erstellung des Netzstrukturplans.

Meldeorganisation: Um der durch das IT-Sicherheitsgesetz geforderten Meldepflicht nachzukommen, müssen EVU leistungsfähige Meldeorganisationen gestalten. Dafür sind Prozesse, Schnittstellen und Verantwortlichkeiten notwendig. Das durch das BSI vorgestellte Entscheidungsschema, das besagt, wann eine IT-Störung außergewöhnlich und somit meldepflichtig ist,[12] sollte unternehmensintern in konkrete Vorgaben überführt werden. Zudem sollte festgelegt werden, wer an der Klassifizierung von Störungen mitwirkt und welche Stelle verantwortlich und befugt ist, Meldung an das BSI vorzunehmen.

ISMS-Aufbau: Nach ISO/IEC 27001 erfordert ein ISMS die risikoorientierte, ganzheitliche Lenkung der Informationssicherheit im Unternehmen. Dafür müssen verschiedene Managementprozesse definiert werden, beispielsweise zum Risikomanagement, zur Performance-Bewertung des ISMS und zur internen Berichterstattung. Auch müssen Rollen und Verantwortlichkeiten klar festgelegt und eine Leitlinie für Informationssicherheit entwickelt werden. So bildet das ISMS den übergeordneten Rahmen aller Initiativen und Maßnahmen für Informationssicherheit. Bei der Gestaltung der ISMS-Architektur sind stets die Komplexität und Größe des Unternehmens zu berücksichtigen.

Die Ergebnisse der Betroffenheitsanalyse sind Grundlage für die konkrete Architektur der Informationssicherheit im Rahmen des ISMS. Insbesondere die erhobenen Werte und Anlagen fließen in die Prozesse zur Risikoanalyse und -bewertung ein, wobei untersucht wird, welches Risiko für die erfassten Komponenten besteht und wie es behandelt werden soll. Der IT-Sicherheitskatalog nennt hierzu konkrete Schadenskategorien und -szenarien, an denen sich EVU orientieren müssen.

In einer Istanalyse wird im Folgenden geklärt, welche Sicherheitsmaßnahmen bereits vorhanden sind und welche Maßnahmen darüber hinaus noch implementiert werden müssen. Zum einen werden Bereiche erkennbar, in denen bislang gar keine oder nur wenig Sicherheitsmaßnahmen vorhanden sind. Zum anderen bestimmt das erkannte Risikoausmaß und die gewählte Behandlungsoption die Ausgestaltung der Maßnahmen, sodass gegebenenfalls bestehende Regelungen erweitert werden müssen. Die notwendigen Maßnahmen sind unter Berücksichtigung des Stands der Technik auszuwählen und umzusetzen.

Zertifizierung: Bereits bei der Planung und Implementierung des ISMS sollte an die Zertifizierung gedacht werden, insbesondere vor dem zeitlichen Hintergrund. Die Zertifizierung muss bis zum 31. Januar 2018 abgeschlossen sein. Von Beginn der Zertifizierungsprüfung bis Ausstellung des Zertifikats ist für ein mittelgroßes Unternehmen mit zwei bis drei Monaten zu rechnen. Zuvor sollte das ISMS eine gewisse Zeit lang im operativen Betrieb gewesen sein, damit sich die geplanten Prozesse und Aktivitäten mit Leben füllen und das Unternehmen erste Nachweise vorlegen kann. Daher empfiehlt sich der Betriebsstart des ISMS mindestens sechs Monate vor Audit-Beginn.

EVU sollten sich rechtzeitig nach einer Zertifizierungsstelle umsehen. Da BNetzA und DAkkS zum Nachweis der Konformität mit dem IT-Sicherheitskatalog ein neues Zertifizierungsschema nutzen, müssen sich Zertifizierungsanbieter erst akkreditieren lassen. Aufgrund der großen Anzahl an EVU, die eine Zertifizierung nachweisen müssen, wird daher bereits jetzt ein Mangel an Zertifizierern erwartet.

IT-Sicherheit mit Konzept

Der Weg in die Digitalisierung bedingt einen risikobewussten Umgang mit informationstechnischen Systemen, um die individuellen unternehmerischen Ziele, aber auch die allgemeine Versorgungssicherheit zu wahren. Die gesetzliche Regulierung, die in Bereiche eingreift, in denen Unternehmen jahrelang meist freie Hand hatten, und noch dazu enge zeitliche Vorgaben macht, stellt EVU vor große Herausforderungen.

Eine zügige, durchdachte und zielgerichtete Reaktion auf die Vorgaben des IT-Sicherheitsgesetzes und des -katalogs kann Unsicherheiten beseitigen. Energieversorger sollten sich daher mit der Materie vertraut machen – denn meist ist die Ungewissheit darüber, was zu tun ist, der Hauptgrund für den Leidensdruck, der bei manchem Unternehmen entstanden ist. Vor allem kleinere Unternehmen mit begrenzten personellen Ressourcen tun gut daran, ISMS nicht neu zu erfinden, sondern die Unterstützung durch erfahrene Experten zu erwägen. So können sie sich auf ihr Kerngeschäft konzentrieren und alle Chancen der Digitalisierung voll ausnutzen.

Hanna Lurz, Frank Engelking, Wilhelm Dolle

12 Vgl. www.bsi.bund.de/DE/Themen/Industrie_KRITIS/IT-SiG/Neuregelungen_KRITIS/Meldepflicht/meldepflicht_node.html

© 2016 Institut für den öffentlichen Sektor e.V. Alle Rechte vorbehalten.