Bundesnetzagentur

IT-Sicherheitskatalog gemäß § 11 Absatz 1b Energiewirtschaftsgesetz

<u>Stand:</u> Januar 2018

– Konsultationsentwurf –

Inhaltsverzeichnis

A. Einleitung

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. Die Unterstützung durch IKT-Systeme bringt viele Vorteile, mit der wachsenden Abhängigkeit von diesen Systemen gehen jedoch auch Risiken für die Versorgungssicherheit einher. Dies gilt im Besonderen für einen sicheren Netzbetrieb, für den die Bundesnetzagentur mit dem IT-Sicherheitskatalog nach § 11 Absatz 1a Energiewirtschaftsgesetz (EnWG) bereits im August 2015 die Anforderungen zum Schutz gegen Bedrohungen der für einen sicheren Netzbetrieb notwendigen Telekommunikations- und elektronischen Datenverarbeitungssysteme veröffentlicht hat.

Mit Absatz 1b hat der Gesetzgeber eine neue Vorschrift in § 11 EnWG eingefügt, die sich an die Betreiber von Energieanlagen, die als Kritische Infrastruktur nach der BSI-Kritisverordnung bestimmt wurden, richtet. Die Aufnahme von Schutzstandards für diese Energieanlagen ist notwendig, um einen umfassenden Schutz für den Netzbetrieb sicherstellen zu können. Energieanlagen, die mit dem öffentlichen Versorgungsnetz verbunden sind, werden verpflichtet, dort, wo eine Gefährdung für den Netzbetrieb möglich ist, ebenfalls Sicherheitsmaßnahmen zu ergreifen, um die Vorteile moderner IKT auch in Zukunft sicher nutzen zu können.

Ein Schutz ist auch vor dem Hintergrund notwendig, dass sich substanzielle informationstechnische Angriffe auf Anlagenebene i. d. R. gegen mehrere Anlagen gleichzeitig richten werden. Für einen solchen Fall kann daher nicht davon ausgegangen werden, dass angegriffene Energieanlagen einfach durch andere Energieanlagen substituiert werden können. Es ist daher wichtig, dass jede einzelne Anlage über ein entsprechend hohes Schutzniveau verfügt, um nicht Teilziel oder gar Werkzeug von Angriffen auf die Strom- oder Gasversorgung zu werden.

Der vorliegende IT-Sicherheitskatalog für Energieanlagen nach § 11 Absatz 1b EnWG beinhaltet die Anforderungen an die Betreiber, um einen angemessenen Schutz gegen Bedrohungen für Telekommunikations- und EDV-Systeme, die für einen sicheren Anlagenbetrieb notwendig sind, zu etablieren.

B. Schutzziele

Der vorliegende IT-Sicherheitskatalog enthält Anforderungen zur Gewährleistung eines angemessenen Schutzes gegen Bedrohungen für Telekommunikations- und elektronische Datenverarbeitungssysteme, die für einen sicheren Anlagenbetrieb notwendig sind.

I. Allgemeine Schutzziele

Ein angemessener Schutz gegen Bedrohungen für Telekommunikations- und elektronische Datenverarbeitungssysteme, die für einen sicheren Anlagenbetrieb notwendig sind, ist insbesondere durch die Auswahl geeigneter, angemessener und dem allgemein anerkannten Stand der Technik entsprechender Maßnahmen zur Realisierung der folgenden Schutzziele[1] aus dem Bereich der Informationssicherheit zu erreichen:

- die Sicherstellung der **Verfügbarkeit** der zu schützenden Systeme und Daten,
- die Sicherstellung der **Integrität** der verarbeiteten Informationen und Systeme,
- die Gewährleistung der **Vertraulichkeit** der mit den betrachteten Systemen verarbeiteten Informationen.

Verfügbarkeit bedeutet, dass die zu schützenden Systeme und Daten auf Verlangen einer berechtigten Einheit zugänglich und nutzbar sind. Es muss sichergestellt werden, dass Daten, Systeme und (informationstechnische) Netzwerke, die für die Erbringung der zugesicherten Leistung oder die Einhaltung anderer Anforderungen an die Energieanlagen in Bezug auf die Netzstabilität notwendig sind, im für die Gewährleistung der Energieversorgung benötigten Umfang zur Verfügung stehen.

Integrität bedeutet zum einen die Richtigkeit und Vollständigkeit der verarbeiteten Daten und zum anderen die korrekte Funktionsweise der Systeme. Das bedeutet, dass die Erbringung der zugesicherten Leistung oder die Einhaltung anderer Anforderungen an die Energieanlagen in Bezug auf die Netzstabilität durch eine korrekte und vollständige Übertragung, Speicherung sowie Verarbeitung von Daten sichergestellt werden muss.

Unter **Vertraulichkeit** wird der Schutz der Systeme und Daten vor unberechtigtem Zugriff durch Personen oder Prozesse verstanden. Es muss sichergestellt werden, dass Daten, deren Offenlegung die Erbringung der zugesicherten Leistung oder die Einhaltung anderer Anforderungen an die Energieanlagen in Bezug auf die Netzstabilität gefährden würde, unberechtigten Personen oder Institutionen nicht bekannt werden.

[1] Vgl. DIN 27000, S. 13, 17.

Die Angemessenheit der durchzuführenden Maßnahmen ist vom individuellen Schutzbedarf der jeweiligen Anlage unter Berücksichtigung der allgemeinen und besonderen Schutzziele abhängig. In die Ermittlung des individuellen Schutzbedarfs sind sowohl Risiken für den Anlagenbetrieb als auch Risiken für die Sicherheit verbundener Energieversorgungsnetze einzubeziehen.

Die Verantwortung für die Erfüllung der Schutzziele trägt der Anlagenbetreiber, auch wenn er sich hierzu Dritter bedient. Er stellt die Erarbeitung, Kommunikation, Durchführung und Dokumentation der zur Umsetzung der Schutzziele getroffenen Maßnahmen innerhalb der Organisation sicher.

II. Besondere Schutzziele nach Anlagentyp

Energieanlagen müssen jederzeit so betrieben werden, dass von ihnen keine Gefährdung für den sicheren Netzbetrieb ausgeht.

Dabei sind insbesondere die nachfolgenden besonderen Schutzziele für die jeweiligen Anlagentypen zu erfüllen.

1. Erzeugungsanlagen (gemäß Anhang 1, Teil 3, Nr. 1.1.1 BSI-KritisV)

Bereitstellung von elektrischer Leistung entsprechend den kommunizierten Fahrplänen und vertraglichen Verpflichtungen im Rahmen der Maßnahmen gemäß § 13 Abs. 1 EnWG.

Bereitstellung von elektrischer Leistung entsprechend der Anforderung des Übertragungsnetzbetreibers gemäß § 13 Abs. 2 EnWG und der Anforderung des Verteilnetzbetreibers gemäß § 13 Abs. 2 i. V. m. § 14 Abs. 1 EnWG.

Bereitstellung von elektrischer Leistung zur Deckung des lebenswichtigen Bedarfs an Elektrizität entsprechend den Verfügungen des Lastverteilers gemäß § 1 Abs. 1 Nr. 1 Elektrizitätssicherungsverordnung i. V. m. § 1 Abs. 1 Energiesicherungsgesetz.

Gewährleistung der Schwarzstartfähigkeit, sofern technisch möglich und vertraglich mit dem Übertragungsnetzbetreiber vereinbart, sowie die Unterstützung des Übertragungsnetzbetreibers beim Netzwiederaufbau.

2. Gasspeicher (gemäß Anhang 1, Teil 3, Nr. 2.1.2 BSI-KritisV)

Bereitstellung von Speicherkapazität entsprechend den kommunizierten Anweisungen des Dispatchings und Ein- und Ausspeisung von Gasmengen entsprechend den vertraglichen Verpflichtungen im Rahmen der Maßnahmen gemäß § 16 Abs. 1 EnWG.

Ein- und Ausspeisung von Gasmengen entsprechend den Anforderungen des Fernleitungsnetzbetreibers gemäß § 16 Abs. 2 EnWG und den Anforderungen des Verteilernetzbetreibers gemäß § 16 Abs. 2 i. V. m. § 16a EnWG.

Ein- und Ausspeisung von Gasmengen zur Deckung des lebenswichtigen Bedarfs an Gas entsprechend den Verfügungen des Lastverteilers gemäß § 1 Abs. 1 Nr. 1 Gassicherungsverordnung i. V. m. § 1 Abs. 1 Energiesicherungsgesetz.

C. Geltungsbereich

Betreiber von Energieanlagen, die durch Inkrafttreten der Rechtsverordnung gemäß § 10 Absatz 1 des BSI-Gesetzes (BSI-Kritisverordnung) vom 14. August 2009 (BGBl. I S. 2821) in der jeweils geltenden Fassung als Kritische Infrastruktur bestimmt wurden und an ein Energieversorgungsnetz angeschlossen sind, haben einen angemessenen Schutz gegen Bedrohungen für Telekommunikations- und elektronische Datenverarbeitungssysteme (TK- und EDV-Systeme) zu gewährleisten, die für einen sicheren Anlagenbetrieb notwendig sind. Die Aufnahme von Schutzstandards für diese Energieanlagen ist notwendig, um einen umfassenden Schutz für den Netzbetrieb sicherstellen zu können.

Um die Sicherheitsanforderungen für die verschiedenen Betreiber von Energieanlagen im Einzelnen zu ermitteln, bedarf es einer an den Schutzzielen ausgerichteten Vorgehensweise zur Identifizierung der betroffenen TK- und EDV-Systeme.

Der Geltungsbereich des vorliegenden IT-Sicherheitskatalogs umfasst alle zentralen und dezentralen Anwendungen, Systeme und Komponenten, die für einen sicheren Anlagenbetrieb notwendig sind. Die Ermittlung der im Einzelfall betroffenen Anwendungen, Systeme und Komponenten erfolgt durch den jeweiligen Anlagenbetreiber selbst unter Beachtung der in diesem IT-Sicherheitskatalog vorgegebenen Kriterien und mit Blick auf das Ziel eines umfassenden Schutzes für den Netzbetrieb. Werden Anwendungen, Systeme und Komponenten, die der Anwendung des Katalogs unterliegen, nicht vom Anlagenbetreiber selbst betrieben, sondern von Dritten, beispielsweise im Rahmen von Outsourcing, so ist die Anwendung und Umsetzung des Katalogs durch entsprechende Vereinbarungen sicherzustellen. Die volle Verantwortung in Bezug auf die Einhaltung des Katalogs bleibt dabei beim Betreiber der Energieanlage.

Dementsprechend haben Betreiber von Energieanlagen, die durch die BSI-Kritisverordnung als Kritische Infrastruktur bestimmt wurden und an ein Energieversorgungsnetz angeschlossen sind, alle in der Energieanlage eingesetzten TK- und EDV-Systeme in eine der im Folgenden genannten Zonen 1 bis 6 einzuteilen.[2] Dabei sind sowohl Systeme, die für die Prozessführung und im Leitstand eingesetzt werden, als auch Büro- und Verwaltungsinformationssysteme zu berücksichtigen.

Zone 1:

Zwingend notwendig für den sicheren Betrieb der Energieanlage:

[2] Unter dem hier verwendeten Begriff der Zone ist nicht eine Netzsegmentierung zu verstehen, sondern eine Klassifizierung von Anwendungen, Systemen und Komponenten einer Energieanlage hinsichtlich ihrer Bedeutung für den sicheren Anlagenbetrieb.

- Fokus auf Verfügbarkeit des Systems bzw. der Funktionalität und auf die Integrität der Messungen und Signale zum Schutz von Menschen, Anlage und Umwelt
- Manipulation von Daten führt direkt zu Auswirkungen auf die angesteuerten Anlagenteile
- Keine Ausfalltoleranz – Anlage bzw. Anlagenteile schalten sich bei Fehlfunktionen umgehend ab

Zone 2:

Dauerhaft notwendig für den Betrieb der Energieanlage:

- Fokus auf Integrität der Messungen, Signale und Daten und der Verfügbarkeit des Systems bzw. der Funktion
- Manipulation der Daten kann indirekt zu falschen Bedienhandlungen führen
- Ausfalltoleranz: wenige Minuten bis eine Stunde – Anlage kann kurzfristig mit erhöhtem personellen Einsatz zur manuellen Überprüfung von Funktionalitäten, zur manuellen Steuerung oder Hand-Nachrechnung von Werten ohne Beeinträchtigung von Menschen, Anlage und Umwelt weiter betrieben werden

Zone 3:

Notwendig für den (effizienten) Betrieb der Energieanlage und zur Erfüllung gesetzlicher Anforderungen:

- Fokus auf Integrität der Daten
- Manipulation der Daten kann indirekt Auswirkungen auf die optimale Fahrweise der betriebenen Anlagen haben (Wirtschaftlichkeit, Umweltverträglichkeit, Verschleiß) und zu Rückwirkungen auf den sicheren Netzbetrieb führen
- Ausfalltoleranz: wenige Stunden – Anlage fährt mit reduziertem Wirkungsgrad, Netzdienstleistungen entfallen, Daten der Energieanlage sind extern nicht verfügbar, Instandhaltung ist erschwert oder nicht mehr möglich

Zone 4:

Bedingt notwendig für den kontinuierlichen Betrieb der Energieanlage:

- Schutzbedarf dieser Systeme muss spezifisch ermittelt werden
- Ausfalltoleranz: wenige Tage – sicherer Analgenbetrieb bei Ausfall weiterhin möglich

Zone 5:

Notwendig für die organisatorischen Prozesse der Energieanlage:

- Schutzbedarf dieser Systeme muss spezifisch ermittelt werden
- Ausfalltoleranz: eine Woche – sicherer Anlagenbetrieb bei Ausfall weiterhin möglich

Zone 6:

Bedingt notwendig für die Organisation der Prozesse der Energieanlage:

- Schutzbedarf dieser Systeme muss spezifisch ermittelt werden
- Ausfalltoleranz: eine Woche – sicherer Anlagenbetrieb bei Ausfall weiterhin möglich

Abbildung 1 zeigt eine Zuordnung von Anwendungen, Systemen und Komponenten zu den sechs Zonen. Die Zuordnung ist nicht abschließend und individuell zu ergänzen.

Abbildung 1: Zoneneinteilung von Anwendungen, Systemen und Komponenten in Energieanlagen (Quelle: in Anlehnung an VGB-S175, S. 16)

Können Anwendungen, Systeme und Komponenten mehreren Zonen zugeordnet werden, sind diese jeweils der Zone mit der höheren Bedeutung für den sicheren Anlagenbetrieb zuzuordnen.

D. Sicherheitsanforderungen

I. Informationssicherheits-Managementsystem

Zur Gewährleistung eines angemessenen Sicherheitsniveaus für TK- und EDV-Systeme, die für einen sicheren Anlagenbetrieb notwendig sind, ist die bloße Umsetzung von Einzelmaßnahmen, wie zum Beispiel der Einsatz von Antivirensoftware, Firewalls usw. nicht ausreichend. Zur Erreichung der Schutzziele ist stattdessen ein ganzheitlicher Ansatz nötig, der kontinuierlich auf Leistungsfähigkeit und Wirksamkeit zu überprüfen und bei Bedarf anzupassen ist.

Einen solchen ganzheitlichen Ansatz stellt ein sog. Informationssicherheits-Managementsystem (ISMS) dar.

> „Ein Managementsystem umfasst alle Regelungen, die für die Steuerung und Lenkung zur Zielerreichung der Institution sorgen. Der Teil des Managementsystems, der sich mit Informationssicherheit beschäftigt, wird als Informationssicherheitsmanagementsystem (ISMS) bezeichnet. Das ISMS legt fest, mit welchen Instrumenten und Methoden das Management die auf Informationssicherheit ausgerichteten Aufgaben und Aktivitäten nachvollziehbar lenkt (plant, einsetzt, durchführt, überwacht und verbessert).“[3]

Dementsprechend haben Betreiber von Energieanlagen, die durch die BSI-Kritisverordnung als Kritische Infrastruktur bestimmt wurden und an ein Energieversorgungsnetz angeschlossen sind, ein ISMS zu implementieren, das den Anforderungen der DIN ISO/IEC 27001 in der jeweils geltenden Fassung genügt.[4] Das ISMS muss mindestens die Anwendungen, Systeme und Komponenten der Zonen 1 bis 3 umfassen.

Eine wesentliche Anforderung der DIN ISO/IEC 27001 ist, dass das ISMS und die damit verbundenen Maßnahmen kontinuierlich auf Wirksamkeit überprüft und im Bedarfsfall angepasst werden. Maßstäbe sind dabei die Schutzziele und die Angemessenheit im Sinne des Abschnitts B. Informationssicherheit und deren Etablierung in einer Organisation darf demnach kein einmaliges Projekt mit definiertem Anfang und Ende sein, sondern muss vielmehr als regelmäßiger Prozess in die Organisationsstrukturen eingebunden werden. Dies kann z.

[3] BSI, S. 13.
[4] Soweit deutsche Übersetzungen der ISO/IEC-Normen in ihrer jeweils aktuellen Fassung noch nicht vorliegen, sind die jeweils aktuellen ISO/IEC-Normen selbst zu berücksichtigen.

B. durch Anwendung des „Plan-Do-Check-Act- Modells“ (PDCA-Modell) für die Prozesse des ISMS erreicht werden. Die Phasen des PDCA-Modells sind in der nachfolgenden Abbildung dargestellt.

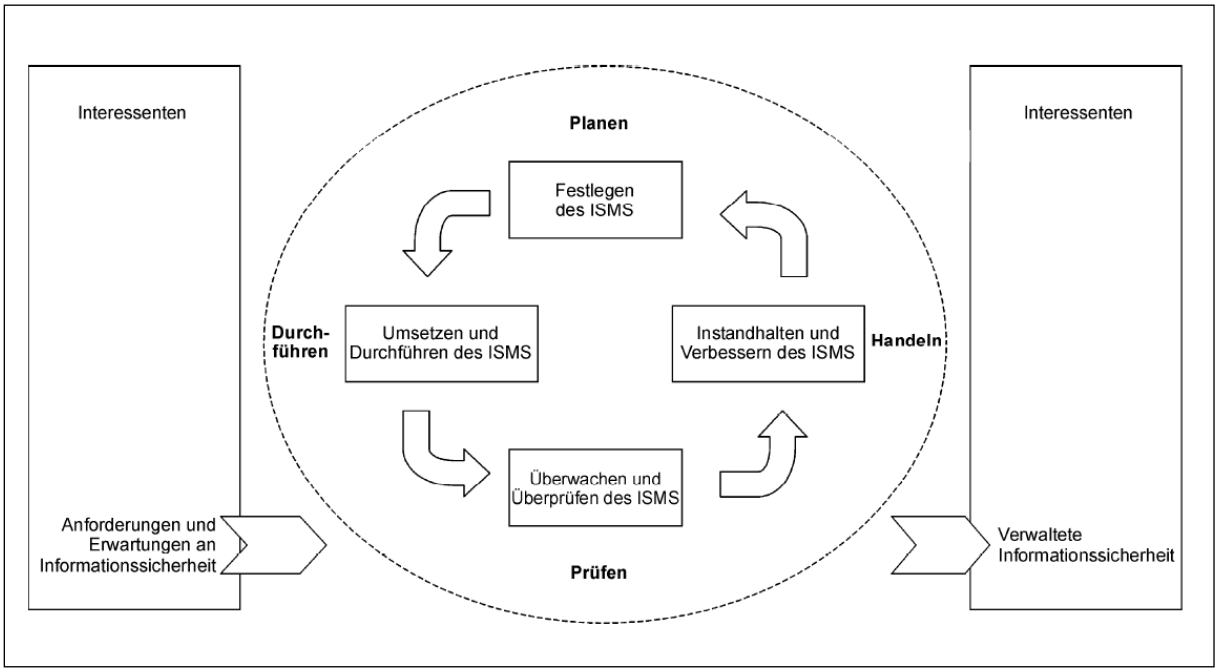

Abbildung: Auf die ISMS-Prozesse angewandtes PDCA-Modell (Quelle: DIN 2008, S. 6)

Die nachfolgende Tabelle 1 enthält eine kurze Erläuterung zu den jeweiligen Phasen.

Phase im PDCA-Modell	**Kurzbeschreibung**
Planen/Plan (Festlegen des ISMS)	Festlegen der ISMS-Leitlinie, -Ziele, -Prozesse und -Verfahren, die für das Risikomanagement und die Verbesserung der Informationssicherheit notwendig sind, um Ergebnisse im Rahmen aller Grundsätze und Ziele einer Organisation zu erreichen.
Durchführen/Do (Umsetzen und Durchführen des ISMS)	Umsetzen und Durchführen der ISMS-Leitlinie, -Maßnahmen, -Prozesse und -Verfahren.
Prüfen/Check (Überwachen und Überprüfen des ISMS)	Einschätzen und ggf. Messen der Prozessleistung an der ISMS-Leitlinie, den ISMS-Zielen und praktischen Erfahrungen, und Berichten der Ergebnisse an das Management zwecks Überprüfung.
Handeln/Act (Instandhalten und Verbessern des ISMS)	Ergreifen von Korrekturmaßnahmen und Vorbeugemaßnahmen, basierend auf den Ergebnissen von internen ISMS-Audits und Überprüfungen des Managements und anderen wesentlichen Informationen, zur ständigen Verbesserung des ISMS.

Tabelle 1: Phasen des PDCA-Modells eines ISMS (Quelle: DIN 2008, S. 7)

II. Sicherheitskategorien und Maßnahmen

Die DIN ISO/IEC 27001 legt Leitlinien und allgemeine Prinzipien für die Initiierung, Umsetzung, den Betrieb und die Verbesserung des Informationssicherheits-Managements in einer Organisation fest.

Für die unterschiedlichen Anlagentypen im Bereich der als Kritische Infrastruktur festgelegten Energieanlagen existieren darüber hinaus Leitlinien und Normen, die als Handlungsempfehlungen bei der Umsetzung des ISMS eine Hilfestellung geben können.

Die in den Leitlinien und Normen genannten Maßnahmen sind nicht per se ungeprüft umzusetzen, sondern immer in Abhängigkeit von ihrer Bedeutung für die Sicherheit der in Abschnitt C. beschriebenen Anwendungen, Systeme und Komponenten unter Berücksichtigung der Ergebnisse der unter D./IV. beschriebenen Risikoeinschätzung.

1. Erzeugungsanlagen (gemäß Anhang 1, Teil 3, Nr. 1.1.1 BSI-KritisV)

Der VGB-Standard „IT-Sicherheit für Erzeugungsanlagen“ (VGB-S-175) gibt über die organisatorischen und prozessualen Anforderungen der DIN-Normen hinaus im Anhang A Handlungsempfehlungen, die sich speziell an die IT-Umgebung der Prozess- und Leittechnik beim Betrieb von Erzeugungsanlagen richten. Bei der Implementierung des ISMS ist daher der Anhang A des VGB-S-175 in der jeweils geltenden Fassung zu berücksichtigen.

Sofern die Handlungsempfehlungen des VGB-S-175 für die Umsetzung der verbindlichen Maßnahmen des Anhangs A der DIN ISO/IEC 27001 nicht ausreichen, sind ergänzend auch die Empfehlungen der DIN ISO/IEC 27002 und der ISO/IEC 27019 in der jeweils geltenden Fassung zu berücksichtigen.[5]

2. Gasspeicher (gemäß Anhang 1, Teil 3, Nr. 2.1.2 BSI-KritisV)

Bei der Implementierung des ISMS sind die Normen DIN ISO/IEC 27002 und ISO/IEC 27019 in der jeweils geltenden Fassung zu berücksichtigen.[6] Die Bundesnetzagentur behält sich vor, etwaige Anpassungen der genannten DIN-Normen in Bezug auf ihre Anwendbarkeit in regelmäßigen Abständen zu überprüfen.

[5] Grundsätzlich sind DIN-Normen zu berücksichtigen. Soweit deutsche Übersetzungen der ISO-Normen in ihrer jeweils aktuellen Fassung noch nicht vorliegen, sind die jeweils aktuellen ISO-Normen selbst zu berücksichtigen. Eine Übersetzung der ISO/IEC 27019:2017 wird für das Frühjahr 2018 erwartet.

[6] Siehe Fn. 5.

III. Ordnungsgemäßer Betrieb der betroffenen IKT-Systeme

Anlagenbetreiber haben nachhaltig sicherzustellen, dass der Betrieb der relevanten Telekommunikations- und Datenverarbeitungssysteme ordnungsgemäß erfolgt. Dies bedeutet insbesondere, dass die eingesetzten IKT-Systeme und IKT-gestützten Verfahren und Prozesse zu jedem Zeitpunkt beherrscht werden und dass technische Störungen als solche erkannt und behoben werden können oder anderweitig deren Behebung sichergestellt werden kann.
Im Rahmen des ISMS müssen auch Risiken durch IKT-basierte Angriffe bewertet und durch geeignete Maßnahmen zum Schutz der relevanten Telekommunikations- und Datenverarbeitungssysteme behandelt werden.

IV. Risikoeinschätzung

Der Anlagenbetreiber muss einen Prozess zur Risikoeinschätzung der Informationssicherheit festlegen. Ziel dieses Prozesses ist es festzustellen, welches Risiko im Hinblick auf die Schutzziele für die von diesem Katalog erfassten Anwendungen, Systeme und Komponenten besteht. Die allgemeinen Anforderungen an diesen Prozess sind in Kapitel 6.1.2. der DIN EN ISO/IEC 27001:2017-06 geregelt. Dabei ist es wichtig, dass die Risikoeinschätzung zu einem entsprechend hohen Schutzniveau für jede einzelne Anlage führt, um nicht Teilziel oder gar Werkzeug von Angriffen auf die Strom- oder Gasversorgung zu werden.

Bei der Bewertung der potenziellen Auswirkungen bei Eintritt der identifizierten Risiken gem. Kapitel 6.1.2 d) 1) sind durch den Anlagenbetreiber folgende Vorgaben zu beachten:

1. Die Risikoeinschätzung hat sich an den Schadenskategorien
    - „kritisch“ (die Schadensauswirkungen können ein existentiell bedrohliches, katastrophales Ausmaß erreichen),
    - „hoch“ (die Schadensauswirkungen können beträchtlich sein) und
    - „mäßig“ (die Schadensauswirkungen sind begrenzt und überschaubar)
    - „gering“ (die Schadensauswirkungen sind vernachlässigbar)

    zu orientieren.

    Für die Anwendungen, Systeme und Komponenten, die für einen sicheren Anlagenbetrieb notwendig sind, ist grundsätzlich von einer Einstufung in die Kategorie „hoch“ auszugehen. Im Einzelnen ist zu prüfen, ob ggf. eine Einstufung als „kritisch“ notwen-

dig ist. Eine vom Grundsatz abweichende Einstufung als „mäßig“ oder sogar als „gering“ ist ausführlich zu begründen und zu dokumentieren.

2. Bei der Einstufung in die Schadenskategorien sind durch den Anlagenbetreiber mindestens die folgenden Kriterien zu berücksichtigen:

    - Beeinträchtigung der Versorgungssicherheit,
    - Einschränkung der Energielieferung,
    - Betroffener Bevölkerungsanteil,
    - Gefährdung für Leib und Leben,
    - Gefährdung für Datensicherheit und Datenschutz durch Offenlegung oder Manipulation,
    - Finanzielle Auswirkungen.

Sicherheitsvorfälle können eine Vielzahl von Ursachen haben. Bei der Ermittlung der Risiken für die Anwendungen, Systeme und Komponenten, die für einen sicheren Anlagenbetrieb notwendig sind, ist zu beachten, dass deren Sicherheit einerseits durch vorsätzliche Handlungen bedroht wird. Hierzu gehören z. B.:

- Gezielte IT-Angriffe,
- Computer-Viren, Schadsoftware,
- Abhören der Kommunikation,
- Diebstahl von Rechnern usw.

Bei der Risikoeinschätzung sind auf der anderen Seite aber auch nicht vorsätzliche Gefährdungen aus den folgenden Kategorien zu berücksichtigen:

- Elementare Gefährdungen,
- Höhere Gewalt,
- Organisatorische Mängel,
- Menschliche Fehlhandlungen,
- Technisches Versagen,
- Versagen oder Beeinträchtigung anderer für die Anlagensteuerung relevanter Infrastrukturen und externer Dienstleistungen,
- Ungezielte Angriffe und Irrläufer von Schadsoftware.

Erläuterungen und praktische Hinweise zur Durchführung von Risikoeinschätzungen sind z. B. in den Standards ISO/IEC 27005, ISO 31000 enthalten.

V. Risikobehandlung

Die Risikobehandlung umfasst die Auswahl geeigneter und angemessener Maßnahmen in Anknüpfung an die nach Kapitel D./IV. erfolgte Risikoeinschätzung. Die allgemeinen Anforderungen an diesen Prozess sind in Kapitel 6.1.3. der DIN EN ISO/IEC 27001:2017-06 geregelt.

Für alle Anwendungen, Systeme und Komponenten, die für einen sicheren Anlagenbetrieb notwendig und nach Kapitel C den Zonen 1 bis 3 zugeordnet sind, sind angemessene und geeignete Maßnahmen zu deren Risikobehandlung zu treffen. Für Anwendungen, Systeme und Komponenten der Zone 1 dürfen die im Rahmen der Risikoeinschätzung ermittelten Risiken nicht akzeptiert werden. Maßnahmen zur Risikobehandlung sind zumindest insoweit umzusetzen, dass lediglich ein als gering zu bewertendes Restrisiko verbleibt.

Sofern Anwendungen, Systeme und Komponenten, die nach Kapitel C den Zonen 1 bis 3 zugeordnet sind, mit Anwendungen, Systemen und Komponenten aus den Zonen 4 bis 6 Informationen austauschen, die für den sicheren Anlagenbetrieb benötigt werden, ist sicherzustellen, dass Verfügbarkeit, Integrität und Vertraulichkeit der Informationen durchgehend gewahrt bleiben. Der Schutzbedarf dieser Informationen richtet sich dabei nach dem Schutzbedarf der Anwendungen, Systeme und Komponenten in der Zone mit der jeweils höheren Bedeutung für den sicheren Anlagenbetrieb.

Hinsichtlich der Geeignetheit einer Maßnahme kann dabei grundsätzlich auf den für den jeweiligen Anwendungsbereich allgemein anerkannten Stand der Technik in der für die Erfüllung der jeweiligen Schutzziele geeigneten Ausprägung zurückgegriffen werden. Soweit dies nicht möglich ist oder aus anderen Gründen abweichende Maßnahmen getroffen werden, ist konkret zu belegen und zu dokumentieren, dass die jeweiligen IKT-Schutzziele dennoch erreicht werden. Bei der Angemessenheit einer Maßnahme ist insbesondere deren technischer und wirtschaftlicher Aufwand zu berücksichtigen. Dieser sollte nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung des sicheren Anlagenbetriebs stehen.

VI. Ansprechpartner IT-Sicherheit

Für die Koordination und Kommunikation der IT-Sicherheit gegenüber der Bundesnetzagentur hat der Anlagenbetreiber einen Ansprechpartner zu benennen, dessen Kontaktdaten der

Bundesnetzagentur mitzuteilen sind. Auf Anfrage soll dieser der Bundesnetzagentur insbesondere zu folgenden Punkten unverzüglich Auskunft geben können:

- Umsetzungsstand der Anforderungen aus dem vorliegenden IT-Sicherheitskatalog
- Aufgetretene Sicherheitsvorfälle sowie Art und Umfang evtl. hierdurch hervorgerufener Auswirkungen (insbesondere in solchen Fällen, die gemäß § 11 Absatz 1c EnWG eine Meldepflicht des Betreibers gegenüber dem BSI auslösen)
- Ursache aufgetretener Sicherheitsvorfälle sowie Maßnahmen zu deren Behebung und zukünftigen Vermeidung

Zudem soll der o. g. Ansprechpartner sicherstellen, dass der Betreiber geeignet an relevante Kommunikationsinfrastrukturen für Lageberichte und Warnmeldungen sowie zur Bewältigung großflächiger IKT-Krisen angebunden ist. Dies kann zum Beispiel durch Teilnahme des Betreibers am UP KRITIS erfolgen (www.upkritis.de).

E. Umsetzungsvorgaben

I. Zertifizierung

Der Anlagenbetreiber ist verpflichtet, die Konformität seines ISMS mit den Anforderungen dieses IT-Sicherheitskatalogs durch ein Zertifikat einer für die Zertifizierung des IT-Sicherheitskatalogs bei der Deutschen Akkreditierungsstelle (DAkkS) akkreditierten unabhängigen Zertifizierungsstelle zu belegen. Die Bundesnetzagentur erarbeitet für solche Zertifizierungsstellen gemeinsam mit der DAkkS ein Konformitätsbewertungsprogramm. Eine Übersicht akkreditierter Stellen zur Zertifizierung des IT-Sicherheitskatalogs kann auf der Internetseite der DAkkS abgerufen werden, sobald entsprechende Akkreditierungsverfahren abgeschlossen sind.

II. Umsetzungsfristen

Zum Nachweis darüber, dass die Anforderungen des vorliegenden IT-Sicherheitskatalogs umgesetzt wurden, hat der Betreiber der Energieanlage der Bundesnetzagentur bis zum XX.XX.XXXX [*1,5 Jahre ab Veröffentlichung des IT-Sicherheitskatalogs*] den Abschluss des Zertifizierungsverfahrens durch Vorlage einer Kopie des Zertifikats mitzuteilen.

Der Ansprechpartner IT-Sicherheit und dessen Kontaktdaten sind der Bundesnetzagentur bis zum xx.xx.xxxx [*2 Monate nach Veröffentlichung des IT-Sicherheitskatalogs*] mitzuteilen. Die Meldung erfolgt über das auf der Internetseite der Bundesnetzagentur bereitgestellte Formular per E-Mail an folgende Adresse:

IT-Sicherheitskatalog@bnetza.de

F. Abweichende Regelungen für Anlagen nach § 7 Absatz 1 des Atomgesetzes

Abweichend von den vorstehenden Regelungen – mit Ausnahme der Verpflichtung zur Benennung eines Ansprechpartners IT-Sicherheit gemäß Kapitel D./VI. – gelten für Anlagen nach § 7 Absatz 1 des Atomgesetzes die nachstehenden Regelungen.

Für die IT-Sicherheit von Anlagen nach § 7 Absatz 1 des Atomgesetzes besteht mit der „Richtlinie für den Schutz von IT-Systemen in kerntechnischen Anlagen und Einrichtungen der Sicherungskategorien I und II gegen Störmaßnahmen oder sonstige Einwirkungen Dritter (SEWD-Richtlinie IT)“ bereits ein anlagenspezifisches Regelwerk, dessen Schutzziele die kerntechnische Sicherheit gewährleisten sollen. Die IT-Sicherheit von Anlagen nach § 7 Absatz 1 des Atomgesetzes muss sich nach § 11 Absatz 1b Satz 1 EnWG jedoch auch an ihrer Bedeutung für den sicheren Netzbetrieb und damit für die allgemeine Versorgungssicherheit orientieren.

Betreiber von Anlagen nach § 7 Absatz 1 des Atomgesetzes sind daher verpflichtet, im Rahmen der Schutzbedarfsfeststellung gemäß SEWD-Richtlinie IT auch die unter B./II./1. genannten besonderen Schutzziele für Erzeugungsanlagen bei der Zuordnung der schutzbedürftigen Anwendungen, Systeme und Komponenten zu den IT-Schutzbedarfsklassen zu berücksichtigen. Diese besonderen Schutzziele sind nachrangig zum Schutzziel der atomaren Sicherheit zu behandeln.

Sofern die besonderen Schutzziele für Erzeugungsanlagen bei der Schutzbedarfsfeststellung berücksichtigt werden, führt die Umsetzung der SEWD-Richtlinie IT zu einem IT-technischen Schutzniveau, welches mit dem in § 11 Abs. 1b S. 1 EnWG geforderten Schutz gegen Bedrohungen für Telekommunikations- und elektronische Datenverarbeitungssysteme, die für einen sicheren Anlagenbetrieb notwendig sind, vergleichbar ist.

Ein angemessener Schutz des Betriebs von Energieanlagen im Sinne von § 11 Absatz 1b Satz 1 EnWG liegt daher für Anlagen nach § 7 Absatz 1 des Atomgesetzes vor, wenn diese den Anforderungen der SEWD-Richtlinie IT entsprechen und bei deren Umsetzung auch die besonderen Schutzziele gemäß Abschnitt B./II./1. berücksichtigen.

Zum Nachweis der Erfüllung der Anforderungen haben Betreiber von Anlagen nach § 7 Absatz 1 des Atomgesetzes erstmalig <u>bis zum 30.06.2019</u> der Bundesnetzagentur eine Bestätigung der für die nukleare Sicherheit zuständigen Genehmigungs- und Aufsichtsbehörden der Länder vorzulegen, aus der hervorgeht, dass die Anforderungen der SEWD-Richtlinie IT vom Betreiber eingehalten werden. Darüber hinaus haben die Betreiber eine verbindliche, von der Geschäftsführung unterzeichnete Erklärung

abzugeben, dass auch die besonderen Schutzziele für Erzeugungsanlagen gemäß Abschnitt B./II./1. bei der Schutzbedarfsfeststellung berücksichtigt wurden. Der Nachweis der Erfüllung der Anforderungen ist jeweils zum 30.06. eines jeden Jahres erneut zu erbringen.

Literaturverzeichnis

BSI BSI: BSI-Standard 100-1: Managementsysteme für Informationssicherheit (ISMS). Version 1.5, 2008 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/BSI-Standard_1001.pdf?__blob=publicationFile&v=1 (Stand: 20.12.2017).

DIN 27000 Informationstechnik – Sicherheitsverfahren – Informationssicherheits-Managementsysteme – Überblick und Terminologie (ISO/IEC 27000:2016); Deutsche Fassung EN ISO/IEC 27000:2017 Berlin, Beuth Verlag, 2017.

DIN 2008 DIN ISO/IEC 27001:2008-09: Informationstechnik – IT-Sicherheitsverfahren – Informationssicherheits-Managementsysteme – Anforderungen (ISO/IEC 27001:2005) Berlin, Beuth Verlag, 2008.