Bundesnetzagentur

IT-Sicherheitskatalog gemäß § 11 Absatz 1b Energiewirtschaftsgesetz

<u>Stand:</u> Dezember 2018

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.[1] Die Aufnahme von Schutzstandards für diese Energieanlagen ist notwendig, um einen umfassenden Schutz für den Netzbetrieb sicherstellen zu können. Betreiber von 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 Bedro-

[1] Für Betreiber von Energieversorgungsnetzen gilt ausschließlich der insoweit abschließende IT-Sicherheitskatalog gemäß § 11 Absatz 1 a EnWG.

hungen 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[2] 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 den sicheren Netzbetrieb 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 den sicheren Netzbetrieb 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 den sicheren Netzbetrieb gefährden würde, unberechtigten Personen oder Institutionen nicht bekannt werden.

[2] Vgl. ISO/IEC 27000, S. 2, 5.

Die Angemessenheit der durchzuführenden Maßnahmen ist vom individuellen Schutzbedarf der zu schützenden TK- und EDV-Systeme 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 hinsichtlich der Schnittstellen zu verbundenen Energieversorgungsnetzen 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 Anlagenkategorien

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 Anlagenkategorien zu erfüllen.

1. Erzeugungsanlagen und Speicheranlagen (gemäß Anhang 1, Teil 3, Nr. 1.1.1 bis 1.1.4 BSI-KritisV)

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

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

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

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

2. Gasförderanlagen und Gasspeicher (gemäß Anhang 1, Teil 3, Nr. 2.1.1 und 2.1.2 BSI-KritisV)

Bereitstellung von Ausspeiseleistung bzw. Speicherkapazität entsprechend den kommunizierten Fahrplänen der Speichernutzer und Ein- und Ausspeisung von Gasmengen entspre-

chend den vertraglichen Verpflichtungen im Rahmen der Maßnahmen gemäß § 16 Absatz 1 EnWG.

Ein- und Ausspeisung von Gasmengen entsprechend den Anforderungen des Fernleitungsnetzbetreibers gemäß § 16 Absatz 2 EnWG und den Anforderungen des Verteilernetzbetreibers gemäß § 16 Absatz 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 Absatz 1 Nr. 1 Gassicherungsverordnung i. V. m. § 1 Absatz 1 Energiesicherungsgesetz.

C. Geltungsbereich

Betreiber von Energieanlagen, die durch die Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung) vom 22. April 2016 (BGBl. I S. 958), zuletzt geändert durch Artikel 1 der Verordnung vom 21. Juni 2017 (BGBl. I S. 1903), 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.[3] Dabei sind sowohl Systeme, die für die Prozessführung und im Leitstand eingesetzt werden, als auch Büro- und Verwaltungsinformationssysteme zu berücksichtigen.

[3] 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.

Zone 1:

Zwingend notwendig für den sicheren Betrieb der Energieanlage sind diejenigen TK- und EDV-Systeme, die sich durch folgende Eigenschaften auszeichnen:

- Ihr Fokus liegt auf der Verfügbarkeit der Daten und Systeme bzw. der Funktionalität und auf der Integrität der Messungen und Signale zum Schutz von Menschen, Anlage und Umwelt.
- Eine Manipulation von Daten oder Systemen führt direkt zu Auswirkungen auf die angesteuerten Anlagenteile.
- Sie besitzen keine Ausfalltoleranz – Anlage bzw. Anlagenteile schalten sich bei Fehlfunktionen umgehend ab.

Zone 2:

Dauerhaft notwendig für den Betrieb der Energieanlage sind diejenigen TK- und EDV-Systeme, die sich durch folgende Eigenschaften auszeichnen:

- Ihr Fokus liegt auf der Integrität der Messungen, Signale und Daten und der Verfügbarkeit der Daten und Systeme bzw. der Funktionalität.
- Eine Manipulation der Daten oder Systeme kann indirekt zu falschen Bedienhandlungen führen.
- Ihre Ausfalltoleranz liegt bei wenigen Minuten bis einer 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 Betrieb der Energieanlage und zur Erfüllung gesetzlicher Anforderungen sind diejenigen TK- und EDV-Systeme, die sich durch folgende Eigenschaften auszeichnen:

- Ihr Fokus liegt auf der Integrität der Daten.
- Eine Manipulation der Daten oder Systeme kann indirekt Auswirkungen auf die Fahrweise der betriebenen Anlagen haben.
- Ihre Ausfalltoleranz liegt bei wenigen Stunden – Anlage wird nicht planmäßig betrieben, 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 sind diejenigen TK- und EDV-Systeme, die sich durch folgende Eigenschaften auszeichnen:

- Der Schutzbedarf dieser Systeme muss spezifisch ermittelt werden.
- Ihre Ausfalltoleranz liegt bei wenigen Tagen – sicherer Anlagenbetrieb ist bei Ausfall weiterhin möglich.

Zone 5:

Notwendig für die organisatorischen Prozesse der Energieanlage sind diejenigen TK- und EDV-Systeme, die sich durch folgende Eigenschaften auszeichnen:

- Der Schutzbedarf dieser Systeme muss spezifisch ermittelt werden.
- Ihre Ausfalltoleranz liegt bei einer Woche – sicherer Anlagenbetrieb ist bei Ausfall weiterhin möglich.

Zone 6:

Bedingt notwendig für die Organisation der Prozesse der Energieanlage sind diejenigen TK- und EDV-Systeme, die sich durch folgende Eigenschaften auszeichnen:

- Der Schutzbedarf dieser Systeme muss spezifisch ermittelt werden.
- Ihre Ausfalltoleranz liegt bei einer Woche – sicherer Anlagenbetrieb ist 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-Standard, 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 einer Institution sorgen und letztlich zur Zielerreichung führen sollen. Der Teil des Managementsystems, der sich mit der Informationssicherheit beschäftigt, wird als Informationssicherheitsmanagementsystem (ISMS) bezeichnet. Das ISMS legt fest, mit welchen Instrumenten und Methoden die Leitungsebene die auf Informationssicherheit ausgerichteten Aufgaben und Aktivitäten nachvollziehbar lenkt (plant, einsetzt, durchführt, überwacht und verbessert).“[4]

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 EN ISO/IEC 27001 in der jeweils geltenden Fassung genügt.[5] Das ISMS muss mindestens die Anwendungen, Systeme und Komponenten der Zonen 1 bis 3 umfassen.

Eine wesentliche Anforderung der DIN EN 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

[4] BSI-Standard 200-1, S. 15.
[5] 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.

z. 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 2 dargestellt.

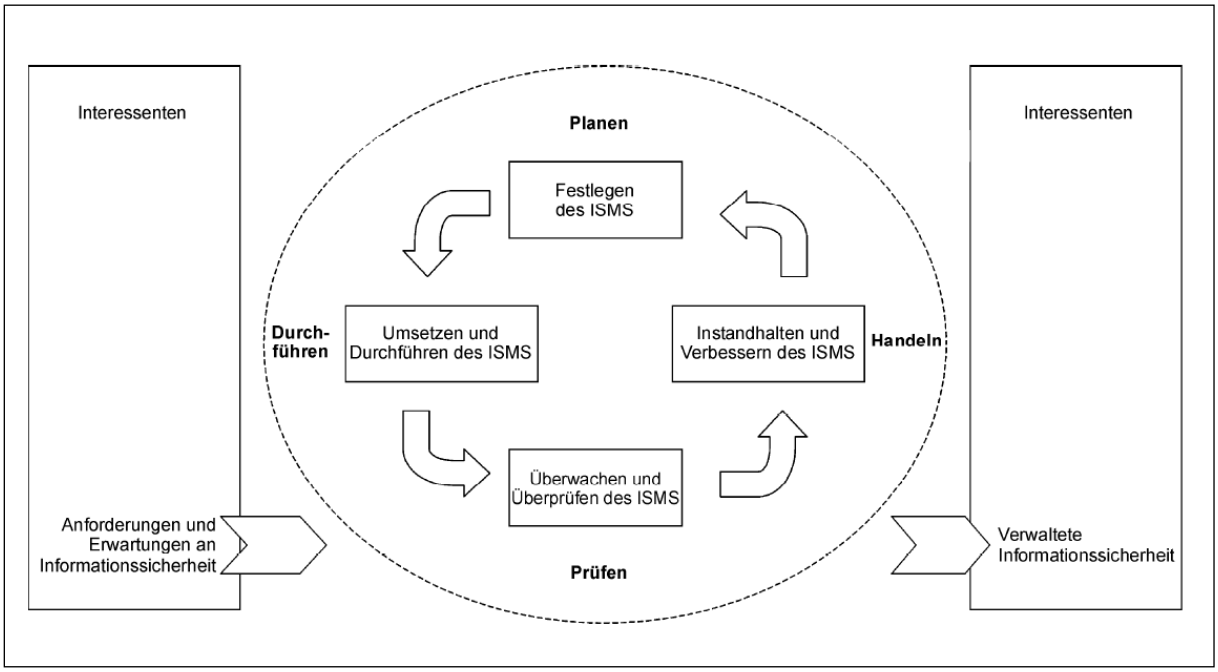

Abbildung 2: Auf die ISMS-Prozesse angewandtes PDCA-Modell (Quelle: DIN ISO/IEC 27001:2008, S.6)

Die nachfolgende Tabelle 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; 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: Phasen des PDCA-Modells eines ISMS (Quelle: DIN ISO/IEC 27001:2008, S. 7)

II. Sicherheitskategorien und Maßnahmen

Die DIN EN ISO/IEC 27001 legt Anforderungen und allgemeine Prinzipien für die Initiierung, Umsetzung, den Betrieb und die Verbesserung des Informationssicherheits-Managements in einer Organisation fest. Darauf aufbauend formuliert die DIN EN ISO/IEC 27002 Umsetzungsempfehlungen für die verbindlichen Maßnahmen des Anhangs A der DIN EN ISO/IEC 27001. Die DIN EN ISO/IEC 27019 erweitert diese in verschiedenen Punkten um Besonderheiten im Bereich der Prozesssteuerung der Energieversorgung.

Bei der Implementierung des ISMS sind daher die Normen DIN EN ISO/IEC 27002 und DIN EN ISO/IEC 27019 in der jeweils gültigen 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.**

Die in den 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.

Für einige Anlagentypen im Bereich der als Kritische Infrastruktur festgelegten Energieanlagen können darüber hinaus der VGB-Standard „IT-Sicherheit für Erzeugungsanlagen“ (VGB-S-175) und das BDEW-Whitepaper „Anforderungen an sichere Steuerungs- und Telekommunikationssysteme“ als Hilfestellung bei der Umsetzung des ISMS dienen. Der VGB-Standard 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. Der BDEW beschreibt in seinem Whitepaper die grundsätzlichen Sicherheitsanforderungen für Steuerungs-und Telekommunikationssysteme in der Energieversorgung und gibt allgemeine Hinweise zu deren Umsetzung.

III. Ordnungsgemäßer Betrieb der betroffenen IKT-Systeme

Anlagenbetreiber haben nachhaltig sicherzustellen, dass der Betrieb der betroffenen Telekommunikations- und elektronischen 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

[6] 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.

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 elektronischen 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 der DIN EN ISO/IEC 27001 geregelt. Dabei ist es wichtig, dass die Risikoeinschätzung zu einem ausreichend 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 sind durch den Anlagenbetreiber folgende Vorgaben zu beachten:

1. Die Risikoeinschätzung hat sich nach den Schadenskategorien

   - „kritisch“ (die Schadensauswirkungen können ein existentiell bedrohliches, katastrophales Ausmaß erreichen),
   - „hoch“ (die Schadensauswirkungen können beträchtlich sein),
   - „mäßig“ (die Schadensauswirkungen sind begrenzt und überschaubar) und
   - „gering“ (die Schadensauswirkungen sind vernachlässigbar)

   zu richten.

   Für die Anwendungen, Systeme und Komponenten, die für einen sicheren Anlagenbetrieb notwendig sind, ist grundsätzlich von einer Einstufung in die Schadenskategorie „hoch“ auszugehen. Im Einzelnen ist zu prüfen, ob ggf. eine Einstufung als „kritisch“ notwendig 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 im Rahmen der Risikoeinschätzung sind durch den Anlagenbetreiber mindestens die folgenden Kriterien zu berücksichtigen:

- Beeinträchtigung der Aufgabenerfüllung (insbesondere im Hinblick auf eine Einschränkung der Energielieferung und den Beitrag zur Versorgungssicherheit),
- 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 insbesondere 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 und 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 der DIN EN ISO/IEC 27001 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 für den sicheren Anlagenbetrieb lediglich ein mittleres akzeptiertes Risikoniveau verbleibt. Das Risikoniveau setzt sich dabei jeweils aus Schadenskategorie und Eintrittswahrscheinlichkeit zusammen.

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 sollte 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. Ansprechpartnerin/Ansprechpartner IT-Sicherheit

Für die Koordination und Kommunikation der IT-Sicherheit gegenüber der Bundesnetzagentur hat der Anlagenbetreiber eine Ansprechpartnerin/einen Ansprechpartner zu benennen, deren/dessen Kontaktdaten der Bundesnetzagentur mitzuteilen sind. Auf Anfrage soll diese/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.

Hiervon unberührt besteht die Pflicht zur Registrierung einer Kontaktstelle[7] gegenüber dem Bundesamt für Sicherheit in der Informationstechnik (BSI) gem. § 8b Absatz 3 BSIG. Über die Kontaktstelle meldet der Betreiber dem BSI IT-Störungen gem. § 11 Absatz 1c EnWG und erhält Unterstützung durch Lageberichte und Warnmeldungen des BSI.

[7] Nähere Hinweise hierzu unter https://mip.bsi.bund.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 31.03.2021

den Abschluss des Zertifizierungsverfahrens durch Vorlage einer Kopie des Zertifikats mitzuteilen.

Die Ansprechpartnerin/der Ansprechpartner IT-Sicherheit und deren/dessen Kontaktdaten sind der Bundesnetzagentur

bis zum 28.02.2019

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 im Geltungsbereich des IT-Sicherheitskatalogs

Abweichend von den vorstehenden Regelungen – mit Ausnahme der Verpflichtung zur Benennung einer Ansprechpartnerin/eines Ansprechpartners IT-Sicherheit gemäß Kapitel D./VI. – gelten für Anlagen nach § 7 Absatz 1 des Atomgesetzes, die durch die BSI-Kritisverordnung als Kritische Infrastruktur bestimmt wurden und an ein Energieversorgungsnetz angeschlossen sind, 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, die durch die BSI-Kritisverordnung als Kritische Infrastruktur bestimmt wurden und an ein Energieversorgungsnetz angeschlossen sind, muss sich nach § 11 Absatz 1b Satz 1 EnWG jedoch auch an ihrer Bedeutung für den sicheren Netzbetrieb und damit an ihrer Bedeutung für die allgemeine Versorgungssicherheit orientieren.

Betreiber von Anlagen nach § 7 Absatz 1 des Atomgesetzes, die durch die BSI-Kritisverordnung als Kritische Infrastruktur bestimmt wurden und an ein Energieversorgungsnetz angeschlossen sind, 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 Anwendung der SEWD-Richtlinie IT zu einem IT-technischen Schutzniveau, welches mit dem in § 11 Absatz 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 bei Anlagen nach § 7 Absatz 1 des Atomgesetzes, die durch die BSI-Kritisverordnung als Kritische Infrastruktur bestimmt wurden und an ein Energieversorgungsnetz angeschlossen sind, vor, wenn keine Risiken offenkundig sind, die die Einhaltung

der Schutzziele nach der SEWD-Richtlinie IT gefährden und auch die besonderen Schutzziele gemäß Abschnitt B./II./1. berücksichtigt werden.

Zum Nachweis der Erfüllung der Anforderungen haben Betreiber von Anlagen nach § 7 Absatz 1 des Atomgesetzes, die durch die BSI-Kritisverordnung als Kritische Infrastruktur bestimmt wurden und an ein Energieversorgungsnetz angeschlossen sind, erstmalig

bis zum 30.06.2019

der Bundesnetzagentur eine Bestätigung der für die nukleare Sicherheit zuständigen Genehmigungs- und Aufsichtsbehörden der Länder vorzulegen, aus der hervorgeht, dass die Schutzziele 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 dieser Anforderungen ist jeweils zum 30.06. eines jeden Jahres erneut zu erbringen.

G. Verweise

Die nachfolgende Auflistung der Normen, Standards und Dokumente, auf die im Anforderungsteil des IT-Sicherheitskatalogs verwiesen wird, gibt grundsätzlich den zum Zeitpunkt der Veröffentlichung dieses IT-Sicherheitskatalogs aktuellen Ausgabestand wieder. Bei der Umsetzung des IT-Sicherheitskatalogs sind die jeweils aktuellen Fassungen zu berücksichtigen.

BSI-Standard 200-1	BSI: BSI-Standard 200-1: Managementsysteme für Informationssicherheit (ISMS). Version 1.0, 2017 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/standard_200_1.pdf?__blob=publicationFile&v=6 (Stand: 11.12.2018).
ISO/IEC 27000	ISO/IEC 27000:2018(E) Information technology – Security techniques – Information security management systems – Overview and vocabulary Fifth edition, 2018-02
DIN ISO/IEC 27001:2008	DIN ISO/IEC 27001:2008-09: Informationstechnik – IT-Sicherheitsverfahren – Informationssicherheits-Managementsysteme – Anforderungen (ISO/IEC 27001:2005) Berlin, Beuth Verlag, 2008.
DIN EN ISO/IEC 27001	DIN EN ISO/IEC 27001:2017-06: Informationstechnik – Sicherheitsverfahren – Informationssicherheitsmanagementsysteme – Anforderungen (ISO/IEC 27001:20013 einschließlich Cor 1:2014 und Cor 2:2015**);** Deutsche Fassung EN ISO/IEC 27001:2017 Berlin, Beuth Verlag, 2017.
DIN EN ISO/IEC 27002	DIN EN ISO/IEC 27002:2017-06 Informationstechnik – Sicherheitsverfahren – Leitfaden für Informationssicherheitsmaßnahmen (ISO/IEC 27002:2013 einschließlich Cor 1:2014 und Cor 2:2015); Deutsche Fassung EN ISO/IEC 27002:2017 Berlin, Beuth Verlag, 2017.

ISO/IEC 27005 ISO/IEC 27005:2018(en)
Information technology — Security techniques — Information security risk management

ISO/IEC 27019 ISO/IEC 27019:2017-10
Information technology - Security techniques - Information security controls for the energy utility industry

ISO 31000 ISO 31000:2018(en)
Risk management — Guidelines

VGB-Standard VGB-Standard IT-Sicherheit für Erzeugungsanlagen
VGB-S-175-00-2014-04-DE
VGB PowerTech e.V., Essen 2014

BDEW Whitepaper (2018) BDEW, Oesterreichs Energie
Whitepaper Anforderungen an sichere Steuerungs- und Telekommunikationssysteme
Vollständig überarbeitete Version 2.0 05/2018
BDEW Bundesverband der Energie- und Wasserwirtschaft e. V.
Oesterreichs E-Wirtschaft
Wien/Berlin, 8. Mai 2018
https://www.bdew.de/media/documents/Awh_20180507_OE-BDEW-Whitepaper-Secure-Systems.pdf (Stand: 11.12.2018)