Bundesnetzagentur

IT-Sicherheitskatalog gemäß § 11 Absatz 1a Energiewirtschaftsgesetz

Stand: August 2015

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. Dies gilt im Besonderen für einen sicheren Netzbetrieb.

Die Unterstützung durch IKT-Systeme bringt viele Vorteile, mit der wachsenden Abhängigkeit von diesen Systemen gehen jedoch auch Risiken für die Versorgungssicherheit einher. Um die Vorteile moderner IKT auch in Zukunft sicher nutzen zu können, ist es daher wichtig, einen angemessenen Schutz gegen Bedrohungen für IKT-Systeme, die für einen sicheren Netzbetrieb notwendig sind, zu etablieren. Dies soll u. a. durch die Umsetzung der Anforderungen des vorliegenden IT-Sicherheitskatalogs erreicht werden.

In Abschnitt B wird der Auftrag an die Bundesnetzagentur zur Erstellung des vorliegenden IT-Sicherheitskatalogs auf Basis des § 11 Abs. 1a EnWG dargestellt. Abschnitt C formuliert die Schutzziele für die unter Abschnitt D als Geltungsbereich definierten Systeme. Abschnitt E enthält konkrete Anforderungen an Netzbetreiber, die unter Berücksichtigung der zuvor genannten Schutzziele umzusetzen sind. Dabei wird auf anerkannte, internationale Standards aus dem Bereich der IT-Sicherheit verwiesen, die bei der Umsetzung der Anforderungen des IT-Sicherheitskatalogs zu beachten sind. Abschnitt F enthält sonstige Forderungen und Fristen für die Umsetzung des IT-Sicherheitskatalogs.

Kernforderung des vorliegenden Sicherheitskatalogs ist die Einführung eines Informationssicherheits-Managementsystems gemäß DIN ISO/IEC 27001 sowie die Zertifizierung durch eine unabhängige hierfür zugelassene Stelle. Des Weiteren soll durch den Netzbetreiber ein Ansprechpartner IT-Sicherheit für die Bundesnetzagentur benannt werden. Die Anforderungen des Sicherheitskatalogs sind unabhängig von der Größe oder der Anzahl der angeschlossenen Kunden von allen Netzbetreibern zu erfüllen, soweit diese über Systeme verfügen, die in den Anwendungsbereich des Sicherheitskatalogs fallen (vgl. Abschnitt D – Geltungsbereich).

B. Rechtliche Grundlagen

§ 11 Absatz 1a Energiewirtschaftsgesetz (EnWG) enthält den Auftrag an die Bundesnetzagentur, im Benehmen mit dem Bundesamt für Sicherheit in der Informationstechnik einen Katalog von Sicherheitsanforderungen zu erstellen zum Schutz gegen Bedrohungen für Telekommunikations- und elektronische Datenverarbeitungssysteme, die für einen sicheren Netzbetrieb notwendig sind.

Mit dieser im Rahmen der EnWG-Novelle 2011 neu eingefügten und durch das Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) vom 17. Juli 2015 novellierten Vorschrift wird die Pflicht zum Betrieb eines sicheren Energieversorgungsnetzes nach § 11 Abs. 1 EnWG konkretisiert. Unter Sicherheit wird in Anlehnung an den in § 1 Absatz 1 EnWG definierten Gesetzeszweck einerseits die technische Anlagensicherheit verstanden, andererseits und vor allem aber auch die allgemeine Versorgungssicherheit. Vor dem Hintergrund einer immer stärkeren Durchdringung des Betriebs von Energieversorgungsnetzen mit Informations- und Kommunikationstechnologie und der damit zunehmenden Bedeutung von IT-Sicherheit umfasst das Ziel der Sicherheit nach dem Willen des Gesetzgebers daher nun auch den angemessenen Schutz gegen Bedrohungen für Telekommunikations- und elektronische Datenverarbeitungssysteme, die für einen sicheren Netzbetrieb notwendig sind.

Ein angemessener Schutz liegt gemäß § 11 Absatz 1a S. 4 EnWG vor, wenn der Katalog der Sicherheitsanforderungen vom Betreiber eines Energieversorgungsnetzes eingehalten wird. Der IT-Sicherheitskatalog stellt insofern einen Mindeststandard dar. Dabei hat der Netzbetreiber insbesondere auch den allgemein anerkannten „Stand der Technik" in Bezug auf die Absicherung der jeweils eingesetzten Systeme zu beachten sowie die allgemeine IKT-Bedrohungslage und die spezifische Bedrohungslage für die eingesetzten Systeme zu berücksichtigen. Dazu sind geeignete, für den jeweiligen Anwendungsbereich formulierte, ggf. branchen- oder sektorspezifische Sicherheitsstandards sowie relevante Empfehlungen, Anwendungsregeln etc. nach jeweils aktuellem Stand heranzuziehen. An der notwendigen Konkretisierung und Ausgestaltung des „Stands der Technik" kann die Branche in den dafür zuständigen Gremien mitwirken.

Das gemäß § 11 Abs. 1a S. 2 EnWG erforderliche Benehmen mit dem Bundesamt für Sicherheit in der Informationstechnik wurde bei der Erstellung des IT-Sicherheitskatalogs hergestellt.

C. Schutzziele

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

Dieses Ziel ist insbesondere durch die Auswahl geeigneter, angemessener und dem allgemein anerkannten Stand der Technik entsprechender Maßnahmen zur Realisierung der folgenden Schutzziele 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. **Integrität** bedeutet zum einen die Richtigkeit und Vollständigkeit der verarbeiteten Daten und zum anderen die korrekte Funktionsweise der Systeme. Unter **Vertraulichkeit** wird der Schutz der Systeme und Daten vor unberechtigtem Zugriff durch Personen oder Prozesse verstanden.[1]

Die Angemessenheit der durchzuführenden Maßnahmen ist vom individuellen Schutzbedarf des jeweiligen Netzbetreibers abhängig. In die Ermittlung des individuellen Schutzbedarfs sind sowohl Risiken für den eigenen Netzbetrieb als auch Risiken bzgl. der Sicherheit verbundener Energieversorgungsnetze einzubeziehen.

Die Verantwortung für die Erfüllung der Schutzziele trägt der Netzbetreiber, 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.

[1] Vgl. DIN 2011, S. 8 f.

D. Geltungsbereich

Der IT-Sicherheitskatalog bezweckt gemäß § 11 Abs. 1a Satz 1 EnWG die Sicherstellung eines angemessenen Schutzes gegen Bedrohungen für Telekommunikations- und elektronische Datenverarbeitungssysteme, die für einen sicheren Netzbetrieb notwendig sind. Um die sich daraus ableitenden Sicherheitsanforderungen für die verschiedenen Betreiber von Energieversorgungsnetzen 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 Netzbetrieb notwendig sind. Enthalten sind demnach zumindest alle TK- und EDV-Systeme des Netzbetreibers, welche direkt Teil der Netzsteuerung sind, d. h. unmittelbar Einfluss nehmen auf die Netzfahrweise. Daneben sind auch TK- und EDV-Systeme im Netz betroffen, die selbst zwar nicht direkt Teil der Netzsteuerung sind, deren Ausfall jedoch die Sicherheit des Netzbetriebs gefährden könnte. Darunter fallen z. B. Messeinrichtungen an Trafo- oder Netzkoppelstationen.

Solange und soweit Messsysteme nach § 21d EnWG zu netzbetrieblichen Zwecken (z. B. Ermittlung von Netzzustandsinformationen, Ermöglichung von Last- und Erzeugungsmanagement u. a.) eingesetzt werden, hat der Netzbetreiber sicherzustellen, dass hinsichtlich dieses Teilbereichs Sicherheitsstandards eingehalten werden, die dem IT-Sicherheitskatalog zumindest gleichwertig sind. Vom Geltungsbereich ausgenommen sind Messsysteme nach § 21d EnWG damit in allen Fällen, in denen sie nicht zu netzbetrieblichen Zwecken eingesetzt werden (z. B. zur Ermittlung von Energieverbräuchen u. a.).
Ungeachtet dieser Differenzierung gelten für alle Messsysteme die besonderen hohen Schutzanforderungen gemäß §§ 21e, 21i EnWG und den auf dieser Basis zu erlassenden Rechtsverordnungen mitsamt der erarbeiteten Schutzprofile und Technischen Richtlinien (z. B. BSI-CC-PP-0073/BSI-CC-PP-0077 und BSI TR-03109).

Die Ermittlung der im Einzelfall betroffenen Anwendungen, Systeme und Komponenten eines Netzes erfolgt durch den jeweiligen Netzbetreiber selbst unter Beachtung der in diesem IT-Sicherheitskatalog vorgegebenen Kriterien. Werden Anwendungen, Systeme und Komponenten, die der Anwendung des Katalogs unterliegen, nicht vom Netzbetreiber selbst betrieben, sondern von Dritten, beispielsweise im Rahmen von Outsourcing oder bei der Aufgabenwahrnehmung der Marktgebietsverantwortlichen im Gasbereich, 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 des Energieversorgungsnetzes.

E. Sicherheitsanforderungen

I. Informationssicherheits-Managementsystem

Zur Gewährleistung eines angemessenen Sicherheitsniveaus für TK- und EDV-Systeme, die für einen sicheren Netzbetrieb 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)."[2]

Dementsprechend haben Netzbetreiber ein ISMS zu implementieren, das den Anforderungen der DIN ISO/IEC 27001 in der jeweils geltenden Fassung genügt[3] und mindestens die unter Abschnitt D beschriebenen Systeme, d. h. Telekommunikations- und EDV-Systeme, die für einen sicheren Netzbetrieb notwendig sind, umfasst.

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 C. 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. 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.

---

[2] BSI, S. 13.

[3] 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.

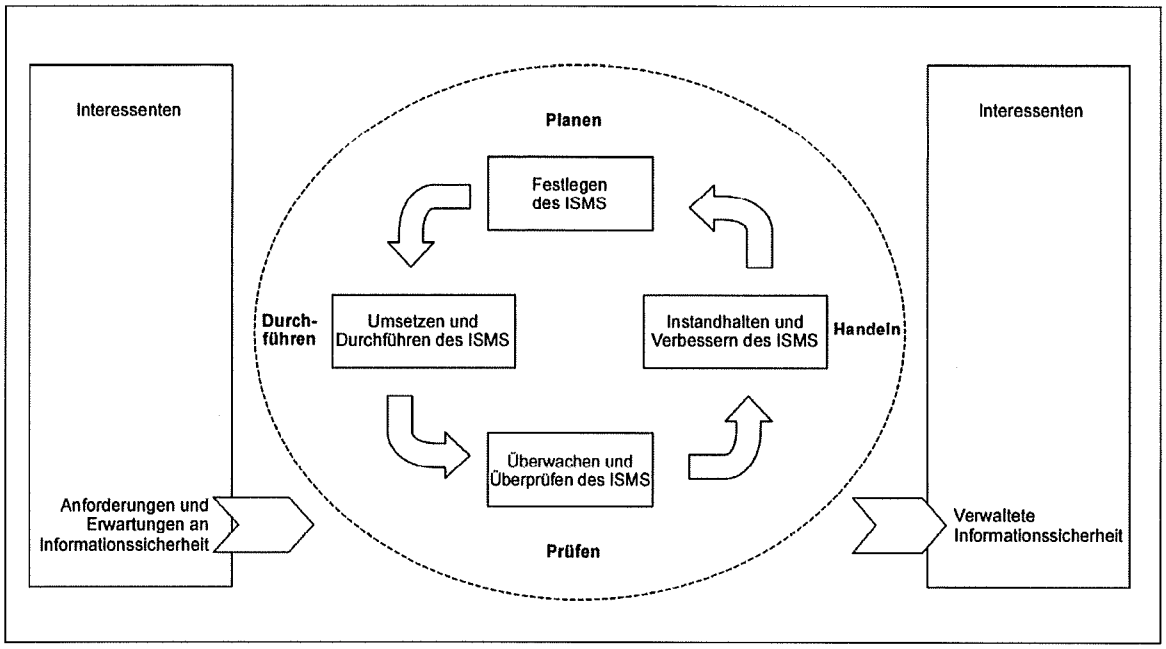

Abbildung: Auf die ISMS-Prozesse angewandtes PDCA-Modell (Quelle: DIN 2008, S. 6)

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

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

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 Vorbeugungsmaßnahmen, basierend auf den Ergebnissen von internen ISMS-Audits und Überprüfungen des Managements und anderen wesentlichen Informationen, zur ständigen Verbesserung des ISMS.

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. Darauf aufbauend formuliert die DIN ISO/IEC 27002 Umsetzungsempfehlungen für die verbindlichen Maßnahmen des Anhangs A der DIN ISO/IEC 27001. Die DIN ISO/IEC TR 27019 (DIN SPEC 27019) erweitert diese in verschiedenen Punkten um Besonderheiten im Bereich der Prozesssteuerung der Energieversorgung.

Bei der Implementierung des ISMS sind daher die Normen DIN ISO/IEC 27002 und DIN ISO/IEC TR 27019 (DIN SPEC 27019) in der jeweils geltenden Fassung zu berücksichtigen[4]. Die Bundesnetzagentur behält sich vor, etwaige Anpassungen der genannten DIN-Normen in Bezug auf ihre Anwendbarkeit in regelmäßigen Abständen zu überprüfen.

Entscheidend für den Umgang mit den Verweisungen und die Umsetzung der sich aus diesem Katalog ergebenden Anforderungen an die IT-Sicherheit ist, diese insbesondere im Hinblick auf die Notwendigkeit für einen sicheren Netzbetrieb anzuwenden. Das heißt 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 D. beschriebenen Anwendungen, Systeme und Komponenten unter Berücksichtigung der Ergebnisse der unter E. V. beschriebenen Risikoeinschätzung.

III. Ordnungsgemäßer Betrieb der betroffenen IKT-Systeme

Netzbetreiber 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.

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

IV. Netzstrukturplan

Der Netzbetreiber hat eine Übersicht über die vom Geltungsbereich des IT-Sicherheitskatalogs betroffenen Anwendungen, Systeme und Komponenten mit den anzutreffenden Haupttechnologien und deren Verbindungen zu erstellen. Die Übersicht ist nach den Technologiekategorien „Leitsystem/Systembetrieb", „Übertragungstechnik/Kommunikation" und „Sekundär-, Automatisierungs- und Fernwirktechnik" zu unterscheiden. Tabelle 2 enthält eine kurze Beschreibung zu den Technologiekategorien sowie einige Beispiele.

Tabelle 2: Technologiekategorien (Quelle: In Anlehnung an BDEW, S. 7 f.)

Technologie-kategorie	**Beschreibung und Beispiele**
Leitsysteme und Systembetrieb	Alle zentralisierten Systeme, die der Netzsteuerung und -überwachung dienen, sowie die hierzu notwendigen unterstützenden IT-Systeme, Anwendungen und zentralen Infrastrukturen. Beispiele: - Zentrale Netzleit- und Netzführungssysteme, - Zentrale Messwerterfassungssysteme, - Systeme zur Überwachung und Steuerung von Netzspeichern, - Datenarchivierungssysteme, - Zentrale Parametrier-, Konfigurations- und Programmiersysteme, - die für den Betrieb der o. g. Systeme notwendigen unterstützenden Systeme.
Übertragungstechnik/Kommunikation	Die in der Netzsteuerung zur Kommunikation eingesetzte Übertragungs-, Telekommunikations- und Netzwerktechnik. Beispiele: - Router, Switches und Firewalls, - Übertragungstechnische Netzelemente, - Zentrale Management- und Überwachungssysteme der Übertragungs-, Telekommunikations- und Netzwerktechnik, - Kommunikationsendgeräte, - Funksysteme.
Sekundär-, Automatisie-	Die prozessnahe Steuerungs- und Automatisierungstechnik, die zugehörigen Schutz- und Sicherheitssysteme sowie fernwirktechnische Kompo-

rungs- und Fernwirktechnik	nenten. Hierzu gehören insbesondere die Technik in den dezentralen Stationen sowie die Automatisierungstechnik in Netzspeicheranlagen. Beispiele: - Steuerungs- und Automatisierungskomponenten, - Leit- und Feldgeräte, - Controller und SPSen inklusive digitaler Sensor- und Aktorelemente, - Schutzgeräte und Sicherheitskomponenten, - Fernwirkgeräte, - Mess- und Zählvorrichtungen.

Die in der Übersicht enthaltenen Anwendungen, Systeme und Komponenten sind in geeigneter Form in einem Netzstrukturplan darzustellen. Die Komplexität des Netzstrukturplans kann durch Gruppenbildung vereinfacht werden (z. B. nach Typ, Konfiguration, Netz, Lokation, Rahmenbedingungen, Anwendungen, Dienste etc.). Ebenso können bei größeren Netzen getrennte Teilpläne sinnvoll sein. Neben den Schnittstellen zwischen den vorgenannten Teilnetzen müssen Schnittstellen zu Teilsystemen, die nicht zu den unter Abschnitt D genannten Teilsystemen gehören oder sich der unmittelbaren Kontrolle des Netzbetreibers (zum Beispiel durch Outsourcing) entziehen, im Netzstrukturplan klar gekennzeichnet und in einer Übersicht definiert werden.
Netzstrukturen sind dabei grundsätzlich danach zu trennen, ob von der Art der dort betriebenen Systeme insgesamt Maßnahmen nach DIN SPEC 27019 greifen oder ob zur Absicherung der in dem IKT-Netz betriebenen Systeme Maßnahmen nach DIN ISO/IEC 27002 anzuwenden sind.

V. Risikoeinschätzung

Der Netzbetreiber muss einen Prozess zur Risikoeinschätzung der Informationssicherheit festlegen. Ziel dieses Prozesses ist es festzustellen, welches Risiko in Hinblick auf die Schutzziele für die von diesem Katalog erfassten Komponenten, Systeme und Anwendungen besteht. Die allgemeinen Anforderungen an diesen Prozess sind in Kapitel 6.1.2. der DIN ISO/IEC 27001:2015-3 geregelt.

Bei der Bewertung der potenziellen Auswirkungen bei Eintritt der identifizierten Risiken gem. Kapitel 6.1.2 d) 1) sind durch den Netzbetreiber 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)

   zu orientieren.

   Für die Komponenten, Systeme und Anwendungen, die für einen sicheren Netzbetrieb notwendig sind, ist grundsätzlich von einer Einstufung in die Kategorie „hoch" auszugehen. Im Einzelnen ist zu prüfen, ob ggf. eine Einstufung als „kritisch" notwendig ist. Eine vom Grundsatz abweichende Einstufung als „mäßig" ist ausführlich zu begründen und zu dokumentieren.

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

   - Beeinträchtigung der Versorgungssicherheit,
   - Einschränkung des Energieflusses,
   - Betroffener Bevölkerungsanteil,
   - Gefährdung für Leib und Leben,
   - Auswirkungen auf weitere Infrastrukturen (z. B. vor- und nachgelagerte Netzbetreiber, Wasserversorgung),
   - 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 Komponenten, Systeme und Anwendungen, die für einen sicheren Netzbetrieb 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 Netzsteuerung 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.

VI. Risikobehandlung

Die Risikobehandlung umfasst die Auswahl geeigneter und angemessener Maßnahmen in Anknüpfung an die nach Kapitel V. erfolgte Risikoeinschätzung. Die allgemeinen Anforderungen an diesen Prozess sind in Kapitel 6.1.3. der DIN ISO/IEC 27001:2015-3 geregelt.

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 Netzbetriebs stehen.

VII. Ansprechpartner IT-Sicherheit

Für die Koordination und Kommunikation der IT-Sicherheit gegenüber der Bundesnetzagentur hat der Netzbetreiber 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

- 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).

Bei der Bestimmung des Ansprechpartners sind – soweit einschlägig – die Vorschriften des Sicherheitsüberprüfungsgesetzes (SÜG) und der Sicherheitsüberprüfungsfeststellungsverordnung (SÜFV) zu beachten.

F. Umsetzungsvorgaben

I. Zertifizierung

Der Netzbetreiber ist verpflichtet, die Konformität seines ISMS mit den Anforderungen dieses IT-Sicherheitskatalogs durch ein Zertifikat zu belegen. Die Bundesnetzagentur erarbeitet hierzu gemeinsam mit der Deutschen Akkreditierungsstelle (DAkkS) ein entsprechendes Zertifikat auf der Basis von DIN ISO/IEC 27001. Die Zertifizierung muss durch eine unabhängige und für die Zertifizierung akkreditierte Stelle durchgeführt werden. 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 Netzbetreiber der Bundesnetzagentur bis zum 31.01.2018 den Abschluss des Zertifizierungsverfahrens durch Vorlage einer Kopie des Zertifikats mitzuteilen.

Der Ansprechpartner IT-Sicherheit und dessen Kontaktdaten sind der Bundesnetzagentur bis zum 30.11.2015 mitzuteilen. Die Meldung erfolgt über das auf der Internetseite der Bundesnetzagentur bereitgestellte Formular per E-Mail an folgende Adresse:

IT-Sicherheitskatalog@bnetza.de

Literaturverzeichnis

BDEW BDEW; Oestereichs E-Wirtschaft: Ausführungshinweise zur Anwendung des Whitepaper „Anforderungen an sichere Steuerungs- und Telekommunikationssysteme“: Oestereichs Energie und bdew Best Practice Papier. Version 1.0 Wien und Berlin: 2011.

BSI BSI: BSI-Standard 100-1: Managementsysteme für Informationssicherheit (ISMS). Version 1.5, https://www.bsi.bund.de/DE/Publikationen/BSI_Standard/it_grundschutzstandards.html, 2008, 21.06.2013.

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

DIN 2011 DIN; DIN ISO/IEC 27000:2011-07: Informationstechnik – IT-Sicherheitsverfahren – Informationssicherheits-Managementsysteme – Überblick und Terminologie (ISO/IEC 27000:2009). Berlin: Beuth Verlag, 2011.