BDEW Bundesverband der Energie- und Wasserwirtschaft e. V.
Reinhardtstraße 32
10117 Berlin

www.bdew.de

Branchenspezifischer Sicherheitsstandard für

Anlagen oder Systeme zur Steuerung / Bündelung elektrischer Leistung (B3S Aggregatoren)

Nach § 8a Abs. 2 BSI-Gesetz

Version: 1.1
Stand: 15.02.2021

Inhalt

Einleitung 4
1 GELTUNGSBEREICH UND SCHUTZZIELE 7
1.1 Geltungsbereich 7
1.1.1 Mindestgeltungsbereich 7
1.1.2 Geltungsbereich umfasst auch extern erbrachte Leistungen 10
1.1.3 Abgrenzung zum IT-Sicherheitskatalog nach § 11 Abs. 1a EnWG für Betreiber von Energieversorgungsnetzen 10
1.2 Informationssicherheitsmanagementsystem (ISMS) 11
1.3 Gesetzlicher und regulatorischer Rahmen 11
1.4 KRITIS-Schutzziele / Branchenspezifische Schutzziele 11
1.5 IT-Schutzziele 12
2 BRANCHENSPEZIFISCHE GEFÄHRDUNGSLAGE 14
2.1 All-Gefahrenansatz und branchenspezifische Relevanz von Bedrohungen und Schwachstellen 14
2.2 Benennung der Bedrohungen und Schwachstellen 16
3 RISIKOBEHANDLUNG (Risikomanagement) 19
3.1 Geeignete Behandlung aller für den kDL-Teilprozess relevanten Risiken 19
3.2 Beschränkung der Behandlungsalternativen für Risiken 20
3.3 Berücksichtigung von Abhängigkeiten bei der Risikoanalyse 20
3.4 Änderung der allgemeinen und branchenspezifischen Gefährdungslage 21
4 ANGEMESSENE VORKEHRUNGEN (MASSNAHMEN) 22
4.1 Angemessenheit der Maßnahmen 22
4.2 Eignung von Maßnahmen 22
5 ABZUDECKENDE THEMEN 23
5.1 Abdeckung relevanter Themen 23
5.2 Informationssicherheitsmanagementsystem (ISMS) 23
5.3 Risikoanalysemethoden 23
5.4 Continuity und Notfall-Management 24
5.5 Asset Management 24
5.6 Bauliche / physische Sicherheit 25

5.7 Personelle und organisatorische Sicherheit 26
5.8 Branchenspezifische Technik 27
5.9 Vorfallserkennung und –bearbeitung 28
5.10 Überprüfung im laufenden Betrieb 29
5.11 Externe Informationsversorgung und Unterstützung 30
5.12 Lieferanten, Dienstleister und Dritte 30
5.13 Technische Informationssicherheit 31
6 NACHWEISBARKEIT DER UMSETZUNG 32
7 Literaturverzeichnis 33
8 Anhang A – Maßnahmen Technische Informationssicherheit 32

Einleitung

Der vorliegende branchenspezifische Sicherheitsstandard (B3S) bildet die spezifischen Mindestanforderungen an Betreiber von Anlagen zur Steuerung / Bündelung elektrischer Leistung (nachfolgend Aggregatoren genannt) in einer prüffähigen Katalogform ab. Die Anforderungen richten sich nach § 8a Abs. 2 zum Nachweis der Erfüllung ihrer Pflichten nach § 8a Abs. 1 Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz). Der B3S geht dabei auf die besondere Charakteristik der Anlagen ein.

Da Aggregatoren in der Lage sind, die Fahrweise einzelner Anlagen zu beeinflussen, haben diese eine unmittelbare Auswirkung auf das Stromnetz. Daraus resultieren spezielle Sicherheitsanforderungen, denen Aggregatoren mit wesentlicher Einflussgröße im Sinne der Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-KritisV) unterliegen. Um bei der Umsetzung des BSI-Gesetzes für Aggregatoren einen einheitlichen Mindeststandard zu gewährleisten und transparente Sicherheitsanforderungen zu definieren wurde der vorliegende B3S entwickelt.

Die technische und organisatorische Charakteristik eines Aggregators wird durch die Kombination unterschiedlicher marktüblicher Informations- und Kommunikations-Technologien (IKT) für die Datenfernübertragung, die Datenverarbeitung sowie die zentrale Steuerung definiert. Im Kern bilden die Anforderungen der ISO/IEC 27001 in der jeweils aktuellen Fassung eine umfassende Anwendungsgrundlage. Der B3S konkretisiert und spezifiziert bei Bedarf diese Anwendungsgrundlage durch geeignete branchenspezifische Ergänzungen.

Dieser B3S für Aggregatoren beinhaltet die Anforderungen an ein Informationssicherheitsmanagementsystem (ISMS) nach ISO/IEC 27001 sowie den internationalen Standards ISO/IEC 27002 und ISO/IEC 27019 in den jeweils gültigen Fassungen, die zusätzlich zu berücksichtigen sind. Der Begriff Informationssicherheit umfasst hierbei auch die IT-Sicherheit im engeren Sinne.

Weitergehende Erläuterungen zu Technologie und Aufgaben von Aggregatoren:

Aggregatoren im Sinne des vorliegenden B3S sind Systeme bzw. die Organisation, die der Zusammenschaltung (Bündelung) sowie der Regelung von Stromerzeugungs- und / oder Verbrauchseinheiten jeglicher Art dient. Dabei ist die jeweilige Technologie zur Bereitstellung elektrischer Leistung in Form von Erzeugungs- oder Verbrauchsanlagen von nachrangiger Bedeutung. Ein Aggregator führt diese Erzeugungs- oder Verbrauchsanlagen zu einem Verbund zusammen, der elektrische Leistung verlässlich bereitstellt bzw. verbraucht. Dabei werden zahlreiche dieser technisch regel- und steuerbaren Anlagen mit unterschiedlichster Technologie (Wind, Solar, Wasser, Biomasse, konventionelle Kraftwerke, schaltbare Lasten, Speicher etc.) über eine Datenanbindung (fernwirktechnische Verbindung) an ein zentrales IT-System angebunden. Primärziel dieser Anbindung ist die 24/7-Online-Datenanbindung mit permanenter Überwachung zur kontinuierlichen Zustandsbestimmung jeder einzelnen technischen Anlage.

Zudem ist die 24/7-Online-Datenanbindung für die Übermittlung von Regelungssignalen bzw. Fahrplänen eine wesentliche Systemfähigkeit. Durch das intelligente Pooling der einzelnen Erzeugungs- und / oder Verbrauchsanlagen bieten diese Anlagen oder Systeme den Zugang zur Direktvermarktung und anderen Märkten, wie z. B. dem Regelenergiemarkt. Ohne Pooling wären diese für einzelne Erzeugungs- und / oder Verbrauchsanlagen durch die gültigen Anforderungen nicht zugänglich.

Aggregatoren, welche Erzeugungs- oder Verbrauchsanlagen bündeln und zentral steuerbar machen, sind beispielsweise im Rahmen der Einführung der Direktvermarktung für Strom aus Erneuerbaren Energien und im Zusammenhang mit der Flexibilitätsvermarktung (Regelenergie, Kurzfristhandel/-optimierung) entstanden. Zudem können mehrere konventionelle Erzeugungs- oder Verbrauchsanlagen durch zentrale Steuerungssysteme aggregiert werden, um wirtschaftlicher und effizienter betrieben zu werden. Weitere Anwendungsgebiete können zum Beispiel im Rahmen der Elektromobilität (Lade-, Fuhrparkmanagement) entstehen. Auf die vorstehend genannte Gruppe von Aggregatoren zielt der vorliegende B3S ab.

Nicht im Fokus des B3S stehen Aggregationsanlagen oder -systeme, welche durch Betreiber von Energieversorgungsnetzen eingesetzt werden, und die für den sicheren Netzbetrieb notwendig sind. Diese fallen stattdessen, wenn sie für den sicheren Netzbetrieb notwendig sind, unter den IT-Sicherheitskatalog der Bundesnetzagentur nach § 11 Abs. 1a Energiewirtschaftsgesetz (EnWG) und haben dementsprechend die Erfüllung der Anforderungen durch ein Zertifikat nach IT-Sicherheitskatalog gegenüber der Bundesnetzagentur nachzuweisen. Ebenfalls nicht in diesem B3S betrachtet werden die einzelnen Erzeugungs- bzw. Verbrauchsanlagen, die vom Aggregator zentral gebündelt und gesteuert werden. Sollte eine Einzelanlage die KRITIS-Schwelle, bspw. für Erzeugungsanlagen überschreiten, fällt sie unter den IT-Sicherheitskatalog der Bundesnetzagentur nach § 11 Abs. 1b EnWG. Der für die Einzelanlage verantwortliche Betreiber muss dann die Erfüllung der dort definierten Anforderungen nachweisen.

Generell haben sich die o.g. Aggregatoren häufig nicht mit dem Geschäftszweck der Erbringung von bestimmten Versorgungsdienstleistungen für die Bevölkerung oder dem Betrieb von Energieversorgungsnetzen bzw. Energieanlagen etabliert, sondern sollen im Wesentlichen eine effiziente Steuerung der angeschlossenen Anlagen sicherstellen. Im Regelfall haben diese Aggregatoren weder einen Versorgungsauftrag noch die dafür notwendigen Arbeitsgrundlagen und Informationen (z.B. Netzzustandsinformationen). Ein Aggregator verfügt zwar über die Sicht auf die durch ihn gebündelten Anlagen, nicht aber zwangsläufig auf Netz- und Systemzustände in den Energieversorgungsnetzen. Hinzu kommt, dass sich Pools von Aggregatoren meist aufgrund von Marktmechanismen, Unternehmensstrategien und -zielen zusammensetzen und nicht primär versorgungsspezifischen Netztopologien folgen. Demnach sollte der Hauptfokus bei der Anwendung des vorliegenden B3S auf der Gefahrenabwehr gegen Missbrauch oder Störfälle beruhen. Eine Ausnahme bilden Aggregatoren, die sogenannte Systemdienstleistungen zur Erbringung von Regelenergie bei den Übertragungsnetzbetreibern anbieten. Diese unterliegen dann

(während der Leistungsvorhaltung bzw. -erbringung) zusätzlichen, spezifischen Sicherheitsanforderungen der Netz- und Systemregeln der deutschen Übertragungsnetzbetreiber (Gridcode bzw. Transmissioncode).

Ein struktureller Sicherheitsaspekt ist die Form der technologischen Anbindung von Daten der einzelnen zu steuernden Anlagen sowie das juristische Verhältnis zwischen den Betreibern der Erzeugungs- oder Verbrauchsanlagen und dem Betreiber des Aggregators. Möglich ist beispielsweise, dass der Aggregator gleichzeitig der Betreiber der zu steuernden Anlagen ist, die aus Gründen der Effizienz und Wirtschaftlichkeit durch zentrale Steuerungssysteme aggregiert werden. Ebenfalls geläufig ist, dass Anlagenbetreiber ihre Erzeugungs- oder Verbrauchsanlagen im Rahmen konkreter und verbindlicher vertraglicher Regelungen bei einem Aggregator in ein sog. Virtuelles Kraftwerk einbinden. Solche Vereinbarungen definieren typischerweise die Art und das Maß der durch das Virtuelle Kraftwerk abrufbaren elektrischen Leistungen sowie individuelle Abruf- bzw. Verhaltensparameter. Diese Parameter werden idealerweise nicht nur auf Seite des Aggregators, sondern auch im System auf Seiten des Anlagenbetreibers vor Ort eingestellt. Das unkontrollierte Ausführen atypischer (nicht vereinbarter) Leistungswerte ist in solchen Fällen limitiert bzw. sollte hier insbesondere auch im Interesse des Anlagenbetreibers auf seiner Seite blockiert werden.

Bisher etablierte Aggregatoren mit KRITIS-Charakter nutzen in der Regel marktgängige Komponenten (wie zum Beispiel industrielle Fernwirktechnik und Supervisory Control and Data Acquisition (SCADA)-Systeme). Neue Aggregatoren mit KRITIS-Charakter nutzen nicht zwangsläufig branchenspezifische Systemkomponenten, sondern setzen zum Beispiel individuell entwickelte Software-Lösungen ein. Da es sich bisher um keinen Massenmarkt im klassisch industriellen Sinne handelt, haben sich auch keine speziellen Branchenlösungen hierfür etabliert – die Vielfalt der verwendeten Komponenten und Techniken, entspricht dem aktuellen Stand der Technik. Zu den verwendeten Dienstleistungen mit der vermutlich größten gemeinsamen Schnittmenge zählen Telekommunikationsdienstleistungen der am Markt etablierten Telekommunikationsanbieter (Internet, Mobilfunk etc.). Insofern besteht die Spezifikation eines branchenspezifischen Sicherheitsstandards weniger in der Definition von konkreten Systemkomponenten und -architekturen sowie Dienstleistungen, sondern vielmehr darin, die verwendeten Betriebsprozesse, die Konfiguration und Anordnung der IT-Systemlandschaft sowie die spezifische Arbeitsorganisation zu betrachten.

1 GELTUNGSBEREICH UND SCHUTZZIELE

1.1 Geltungsbereich

Gemäß § 8a Abs. 2 Satz 1 Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz - **BSIG**) können Betreiber Kritischer Infrastrukturen und ihre Branchenverbände branchenspezifische Sicherheitsstandards (B3S) zur Gewährleistung der Anforderungen nach § 8a Abs. 1 BSIG vorschlagen.

Der B3S für Aggregatoren ist anwendbar für Anlagen nach Anhang 1 Teil 3 Tabelle 1.1.5 der Verordnung zur Bestimmung Kritischer Infrastrukturen (BSI-KritisV), die den in Spalte D genannten Schwellenwert erreichen oder überschreiten und damit als Kritische Infrastruktur (KRITIS) eingestuft worden sind.

Unter Aggregatoren sind Anlagen oder Systeme zur zentralen Steuerung und Fernüberwachung von Energieerzeugungs- oder Verbrauchsanlagen an verschiedenen Standorten zu verstehen. Diese Anlagen oder Systeme zeichnen sich durch das Zusammenschalten von Erzeugungs- und / oder Verbrauchsanlagen aus, wodurch Synergieeffekte frei werden und eine hohe Flexibilität erreicht wird. Die Anlagen tragen somit den Teilprozess der „Steuerung/Bündelung elektrischer Leistung“ (im Folgenden: kDL-Teilprozess SBeL) zur gesamten kritischen Dienstleistung (kDL) Stromversorgung bei.

1.1.1 Mindestgeltungsbereich

Beim kDL-Teilprozess SBeL handelt es sich um eine direkte Einflussnahme auf die Erzeugung oder den Verbrauch und die einhergehende Einspeisung bzw. Entnahme von elektrischer Energie in das bzw. aus dem Netz der öffentlichen Versorgung.

In der Energiebranche sind folgende Auslöser des Steuerungsprozesses häufig in Unternehmen anzutreffen:

- Änderungen am Markt / Marktaktivitäten
- Änderungen der Erzeugung bzw. des Verbrauchs bei Erzeugungs- oder Verbrauchsanlagen (z.B. Energiequellen oder steuerbare Lasten)
- Änderungen der Verfügbarkeiten von Erzeugungs- oder Verbrauchsanlagen
- Einhaltung behördlicher Auflagen
- Anforderungen eines Übertragungs- oder Verteilnetzbetreibers oder eines Geschäfts-/ Vertragspartners im Rahmen der Regelleistungserbringung
- Anforderungen eines Netzbetreibers im Rahmen des Erneuerbare-Energien-Gesetzes (EEG) bzw. EnWG Anforderungen
- Anforderungen eines Übertragungsnetzbetreibers im Rahmen des Redispatch

Hierbei sind nur diejenigen Prozesse sowie der Betrieb der dafür notwendigen Systeme Bestandteil des kDL-Teilprozess SBeL, die zur unmittelbaren Steuerung führen bzw. die für eine

korrekte und planmäßige Steuerung verwendet werden. Diese müssen im Geltungsbereich („Scope“) des gemäß diesem B3S geforderten ISMS mindestens berücksichtigt werden.

Assets im Kontext des B3S ermöglichen die Ausführung von kDL-Teilprozessen SBeL oder der Bereitstellung von Informationen zur Erbringung des kDL-Teilprozess SBeL. Dies können bspw. Gebäude, Geräte, Systeme (Programme), Kommunikation, Daten, Prozesse, Informationen oder Menschen sein.

Der Geltungsbereich des B3S bzw. der Scope beinhaltet damit die Kernprozesse, die der Bündelung und Steuerung mehrerer Erzeugungs- oder Verbrauchsanlagen dienen. Hierbei handelt es sich um die folgenden Prozesse:

- Messung und Überwachung von Erzeugungs- oder Verbrauchsanlagen
- Steuerung und Regelung der elektrischen Leistung von Erzeugungs- oder Verbrauchsanlagen und ihres Einspeise-/Entnahmeverhaltens in das bzw. aus dem Versorgungsnetz

Maßgebliche Infrastrukturen und Ressourcen im Geltungsbereich

Der Geltungsbereich des vorliegenden B3S umfasst alle Bestandteile, die für den Betrieb einer Anlage oder eines Systems zur Steuerung / Bündelung elektrischer Leistung erforderlich und für deren Funktionsweise essenziell sind. Das umfasst insbesondere

- sämtliche zur Messung, Steuerung und Regelung und deren Planung erforderlichen zentralen IT-Infrastrukturen (z.B. SCADA-Applikationen, Regelungs- / Steuerungskomponenten, Energiedaten- und Überwachungssysteme, zentrale Datenbanken mit direkter Anbindung an das Steuer- / Leitsystem)
- sämtliche zum Betrieb der oben genannten IT-Infrastrukturen sowie zur Kommunikation mit den Erzeugungs- oder Verbrauchsanlagen und Netzbetreibern notwendigen zentralen Netzwerke, Firewalls, Gateways, Router etc.
- Betriebsstandorte des Aggregators wie z. B. Leitwarten, Rechenzentren, Technikräume, etc.
- alle für den Betrieb der oben angeführten Systeme erforderlichen Personen bzw. Organisationseinheiten und deren Arbeitsprozesse sowie Arbeitsorganisation (auch externe)
- Verträge (intern, extern)

Die Ermittlung der im Einzelfall betroffenen Anwendungen, Systeme, Prozesse, Komponenten, Betriebsstandorte und Personen bzw. Organisationseinheiten erfolgt durch den jeweiligen Betreiber selbst unter Beachtung der in diesem B3S vorgegebenen Kriterien.

Der Geltungsbereich („Scope“) des gemäß diesem B3S geforderten ISMS muss mindestens die o.g. Anwendungen, Systeme, Komponenten, Betriebsstandorte und Personen bzw. Organisationseinheiten umfassen.

Außerhalb des Geltungsbereichs

Nicht zum Geltungsbereich des vorliegenden B3S gehören dem kDL-Teilprozess SBeL

- vorgelagerte dezentrale Systeme, Prozesse, Standorte und Personal bzw. Organisationseinheiten der Erzeugungs- / Verbrauchsanlagen (z.B. Standorte einzelner Erzeugungs- bzw. Verbrauchsanlagen, die Leittechnik, Netzwerke, Firewalls, Gateways, Router oder Steuerboxen, Wartungspersonal, …) sowie
- nachgelagerte Systeme, Prozesse, Standorte und Personal bzw. Organisationseinheiten des Energiehandels oder der klassischen Marktkommunikation (Applikationen).

Schematische Darstellung des Mindestgeltungsbereichs

Folgende schematisch-generische Darstellung beschreibt den Mindestgeltungsbereich zum B3S exemplarisch. Soweit zum Verständnis erforderlich, ist die Darstellung schriftlich zu beschreiben.

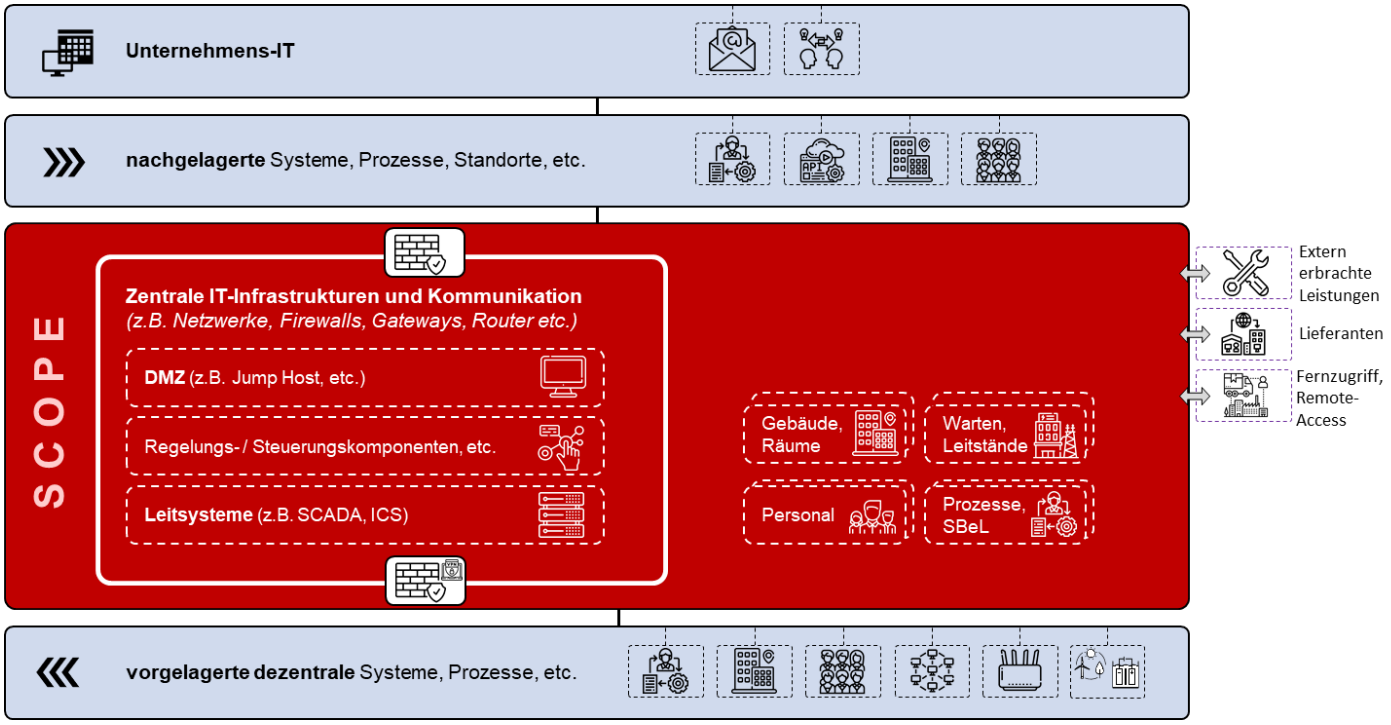

Abbildung 1: Schematische Darstellung des Mindestgeltungsbereichs (Icons: www.flaticon.com)

Dabei sind die Schnittstellen geeignet festzulegen und ausgelagerte Bereiche einer entsprechenden Sicherheitsbetrachtung zu unterziehen. Insbesondere die Abgrenzung des Geltungsbereichs ist für die Eignung des Nachweises sehr wichtig. Aufgrund der Diversität der Einsatzumgebungen gilt es, die Bestandteile des Geltungsbereichs im unternehmensspezifischen Kontext detailliert und umfassend auszugestalten. Das umfasst externe Kommunikationsschnittstellen,

Darstellungen aller relevanten Standorte und Anbindungen, aller ausgelagerten Dienstleistungen, wesentlicher Komponenten im Zusammenspiel mit anderen inklusive nachvollziehbarer Bezeichnungen ihrer Funktionen sowie einer Beschreibung des Bezugs zur Erbringung der kritischen Dienstleistung.

Zur Definition des Geltungsbereichs kann ebenfalls ein detaillierter Netzstrukturplan dienen, der die wesentlichen Bestandteile enthält.

1.1.2 Geltungsbereich umfasst auch extern erbrachte Leistungen

Bei extern erbrachten Leistungen, die dem Verantwortungsbereich des Aggregators unterliegen und für den Betrieb erforderlich sind, ist zur Umsetzung des B3S der Abschluss einer Dienstleistervereinbarung nach A.15 „Supplier Relationship“ ISO/IEC 27001 erforderlich, um sicherzustellen, dass das notwendige informationstechnische Sicherheitsniveau auch dort erbracht werden kann, wo für die Aufrechterhaltung des kDL-Teilprozesses SBeL relevante Teile im Auftrag des Betreibers durch Dritte betrieben werden. Dies umfasst u.a. auch extern erbrachte Telekommunikations-Dienstleistungen sowie das Nichtvorhandensein von Auslagerungen an Dritte.

Umsetzungshinweise, die bei der Ausgestaltung der Maßnahmen unterstützen können:

- - Empfehlungen zur Nutzung von Cloud-Dienstleistungen in Kritischen Infrastrukturen (UP-KRITIS, TAK Cloud-Computing)
- - BDEW-Energie-Info "IT-Sicherheit: Anforderungen bei der Dienstleister- und Herstellerselbstauskunft"

1.1.3 Abgrenzung zum IT-Sicherheitskatalog nach § 11 Abs. 1a EnWG für Betreiber von Energieversorgungsnetzen

Betreiber von Energieversorgungsnetzen sind nach § 11 Abs. 1a EnWG insbesondere verpflichtet, einen angemessenen Schutz gegen Bedrohungen für Telekommunikations- und elektronische Datenverarbeitungssysteme, die für einen sicheren Netzbetrieb notwendig sind, einzuhalten und zu dokumentieren. Im Rahmen des sicheren Netzbetriebs ist es häufig nötig, dass Betreiber von Energieversorgungsnetzen die ans Netz angeschlossenen Anlagen regeln können, um die Netzstabilität zu wahren. Betreiber von Energieversorgungsnetzen betreiben hierzu in manchen Fällen auch Anlagen oder Systeme zur Steuerung/Bündelung elektrischer Leistung (Aggregatoren) im Sinne der BSI-KritisV. Sofern diese für den sicheren Netzbetrieb notwendig sind, fallen diese jedoch nicht unter das BSI-Gesetz, sondern unter § 11 Abs. 1a EnWG, und somit unter den IT-Sicherheitskatalog der Bundesnetzagentur für Energieversorgungsnetze. Gemäß § 8d Abs.2 Nr. 2 BSI-Gesetz unterliegen Betreiber von Energieversorgungsnetzen daher auch nicht § 8a des BSI-Gesetzes, um eine Doppelregulierung zu verhindern.

Für Aggregatoren, die von Betreibern von Energieversorgungsnetzen betrieben werden, und die ausschließlich für den sicheren Netzbetrieb notwendig sind, ist daher nicht der vorliegende B3S einschlägig, sondern der IT-Sicherheitskatalog nach § 11 Abs. 1a EnWG der Bundesnetzagentur.

1.2 Informationssicherheitsmanagementsystem (ISMS)

Der Betreiber muss mindestens für den in Abschnitt 1.1 genannten Geltungsbereich ein Informationssicherheits-Managementsystem gemäß den Anforderungen der ISO/IEC 27001 in der jeweils aktuellen Fassung betreiben.

1.3 Gesetzlicher und regulatorischer Rahmen

Der branchenspezifische gesetzliche Rahmen wird neben § 8a Abs. 1 BSI-Gesetz i. V. m. der BSI-KritisV im Wesentlichen durch die allgemeinen Anforderungen von EnWG und EEG definiert.

Weitere Vorgaben werden durch die Netz- und Systemregeln der deutschen Übertragungsnetzbetreiber (ÜNB), kurz Gridcode oder Transmissioncode genannt, festgelegt. Diese sind ein Regelwerk für den Zugang zum deutschen Verbundnetz. Hier sind die technischen Mindestanforderungen und die Verfahrensweise für den Anschluss und den Parallelbetrieb von Erzeugungsanlagen am Hoch- und Höchstspannungsnetz festgelegt. Die Regeln dienen den Errichtern und Betreibern solcher Anlagen ebenso wie den Netzbetreibern als Planungsgrundlage und Entscheidungshilfe. Die Regeln gelten zwar nur für das deutsche Netz, da dieses aber in das Europäische Verbundnetz eingebunden ist, wurden auch die technischen Anforderungen des Verbandes Europäischer ÜNB (ENTSO-E, vormals UCTE) berücksichtigt. Im Rahmen der Zulassung eines Anbieters von Systemdienstleistungen haben sich die deutschen Übertragungsnetzbetreiber einen gemeinsamen Anforderungskatalog erarbeitet, welchem sich jeder Anbieter im Rahmen der o. g. Zulassung verpflichten muss. Besonders hervorzuheben sind hier die Anforderungen, die sich aus den „Mindestanforderungen an die Informationstechnik des Anbieters für die Erbringung von Regelleistung ergeben“. Diese beinhaltet unter anderem den Nachweis einer Zertifizierung.

1.4 KRITIS-Schutzziele / Branchenspezifische Schutzziele

Die in diesem B3S betrachtete kritische Dienstleistung ist die Versorgung der Allgemeinheit mit Elektrizität (Stromversorgung). Ziel ist es, Störungen aufgrund von IT-Sicherheitsvorfällen zu vermeiden, die die kritische Dienstleistung Stromversorgung in erheblichem Umfang beeinträchtigen. Die Stromversorgung muss grundsätzlich dauerhaft ununterbrochen erfolgen, Blackouts bestmöglich vermieden werden und die Schwarzstartfähigkeit des Gesamtsystems sichergestellt sein. Die informationstechnische Absicherung der Aggregator-Anlagen im Sinne des B3S muss hierbei insbesondere gewährleisten, dass die durch die Aggregatoren jeweils zugesicherten Beiträge (z.B. Bereitstellung/Einspeisung elektrischer Leistung oder Bereitstellung von Regelleistung) zur Stromversorgung und damit auch deren Aufrechterhaltung nicht durch informationstechnische Vorfälle gestört oder unterbrochen werden können. Dieser B3S geht davon aus, dass die betrachteten Aggregator-Anlagen und -Systeme nicht zum Netzwiederaufbau nach Großstörungen wie Blackouts dienen. Sollte dies doch der Fall sein, ist dieser Aspekt in der Risikobetrachtung explizit zu betrachten und die dann notwendigen Maßnahmen umzusetzen.

Das für den kDL-Teilprozess SBeL wesentliche Schutzziel ist somit die planmäßige Erzeugung bzw. der planmäßige Verbrauch von Strom zur Gewährleistung der Versorgungssicherheit. Dies

beinhaltet den planmäßigen Einsatz der durch die Anlage oder das System des Aggregators steuerbaren Erzeugungsanlagen und Lasten. Dasselbe Schutzziel soll in allgemeinen Großkrisen und IT-Krisenlagen angestrebt werden

Generell gilt, dass die informationstechnischen Systeme, Komponenten oder Prozesse der Kritischen Infrastruktur, d. h. IT-Systeme der Prozessdatenverarbeitung zur Messung, Steuerung und Regelung, die für die Funktionsfähigkeit des kDL-Teilprozesses SBeL maßgeblich sind, in unterschiedlichen Lagen geschützt werden.

Von besonderer branchenspezifischer Relevanz sind somit die Bestandteile der Systemlandschaft und Prozesskette, die der Bündelung und Steuerung zahlreicher verteilter Erzeugungs- oder Verbrauchsanlagen an einer zentralen Stelle dienen und dadurch ein hohes Gefährdungspotential bei unplanmäßigen, fahrlässigen oder vorsätzlichen Ein- bzw. Zugriffen sowie Störungen beinhalten. D. h. besonders relevant sind Komponenten, die von einer Stelle ausgehend eine hohe duplizierende Wirkung im Gesamtsystem zulassen (i. d. R. zentrale Systeme und Prozesse mit verteilender Wirkungskette von innen nach außen).

1.5 IT-Schutzziele

Die allgemeinen IT-Schutzziele, die für die Funktionsfähigkeit des kDL-Teilprozesses SBeL maßgeblich sind, werden auf Basis des wesentlichen KRITIS-Schutzziels wie folgt definiert:

- **Vertraulichkeit**

  Es muss sichergestellt werden, dass Informationen, deren Offenlegung die zugesagte Bereitstellung/Einspeisung der durch die Anlage aggregierten elektrischen Leistung oder die Einhaltung anderer relevanter Anforderungen in Bezug auf den sicheren Netzbetrieb in relevantem Umfang gefährden würde, Unberechtigten nicht bekannt werden.

- **Integrität und Authentizität**

  Es muss die Integrität, Authentizität und korrekte Verarbeitung von Informationen sichergestellt werden, deren fehlerhafte, manipulierte oder unvollständige Übertragung, Speicherung oder Verarbeitung die planmäßige Bereitstellung/Einspeisung der durch die Anlage aggregierten elektrischen Leistung in relevantem Umfang beeinträchtigen oder die Einhaltung anderer Anforderungen in Bezug auf den sicheren Netzbetrieb gefährden würde.

- **Verfügbarkeit**

  Es muss sichergestellt werden, dass Informationen, Systeme, Komponenten und Prozesse, die für die planmäßige Bereitstellung/Einspeisung der durch die Anlage aggregierten elektrischen Leistung oder die Einhaltung anderer relevanter Anforderungen in Bezug auf den sicheren Netzbetrieb notwendig sind, im benötigten Umfang zur Verfügung stehen.

Aufbauend auf diesen allgemeinen IT-Schutzzielen sind bei Bedarf im Rahmen des ISMS entsprechend der Abschnitte 4.2 und 6.2 der ISO/IEC 27001 anlagenspezifische Ausprägungen der o.g. Schutzziele abzuleiten bzw. zu erfassen und für informationstechnische Systeme, Kompo-

nenten und Prozesse nach Abschnitt 1.1.2 konsequent zu berücksichtigen. Dabei kann die Gewichtung der anlagenspezifischen IT-Schutzziele für den kDL-Teilprozess SBeL individuell ausfallen.

Der unten dargestellte Prozess skizziert beispielhaft die Ableitung der individuellen, anlagenspezifischen Schutzziele aus dem KRITIS-Schutzziel und den oben genannten allgemeinen IT-Schutzzielen sowie die Integration in einen kontinuierlichen Verbesserungsprozess:

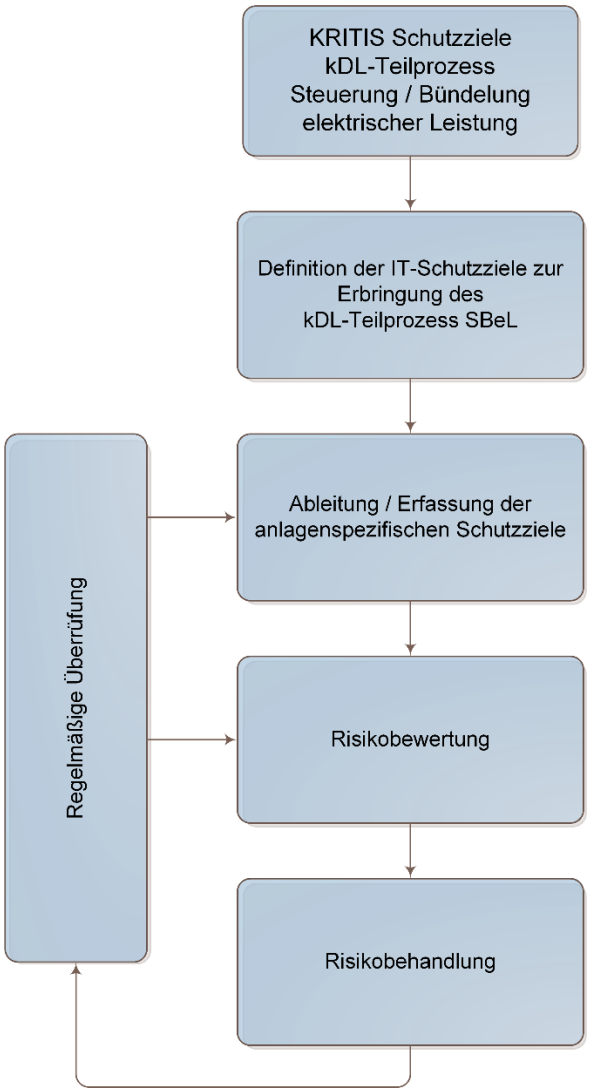

Abbildung 2: Ableitung der individuellen Schutzziele (Quelle: eigene Darstellung)

2 BRANCHENSPEZIFISCHE GEFÄHRDUNGSLAGE

2.1 All-Gefahrenansatz und branchenspezifische Relevanz von Bedrohungen und Schwachstellen

Der Betreiber muss im Rahmen des Risikoanalyseprozesses des ISMS ausdrücklich alle relevanten Bedrohungen und Schwachstellen bzw. Gefährdungen (All-Gefahrenansatz) der maßgeblichen informationstechnischen Systeme, Komponenten oder Prozesse regelmäßig bewerten. Dabei sind mindestens die im folgenden Abschnitt 2.2 genannten Bedrohungen und Schwachstellen bzw. Gefährdungen regelmäßig zu behandeln. Im Rahmen des ISMS ist gemäß ISO/IEC 27001:2013 der Abschnitte 6.1.2 und 8.2 die Relevanz der Gefährdungen innerhalb des Geltungsbereichs hinsichtlich der Auswirkungen auf die Gewährleistung des kDL-Teilprozesses SBeL zu bewerten.

Schematische Darstellung des All-Gefahrenansatzes

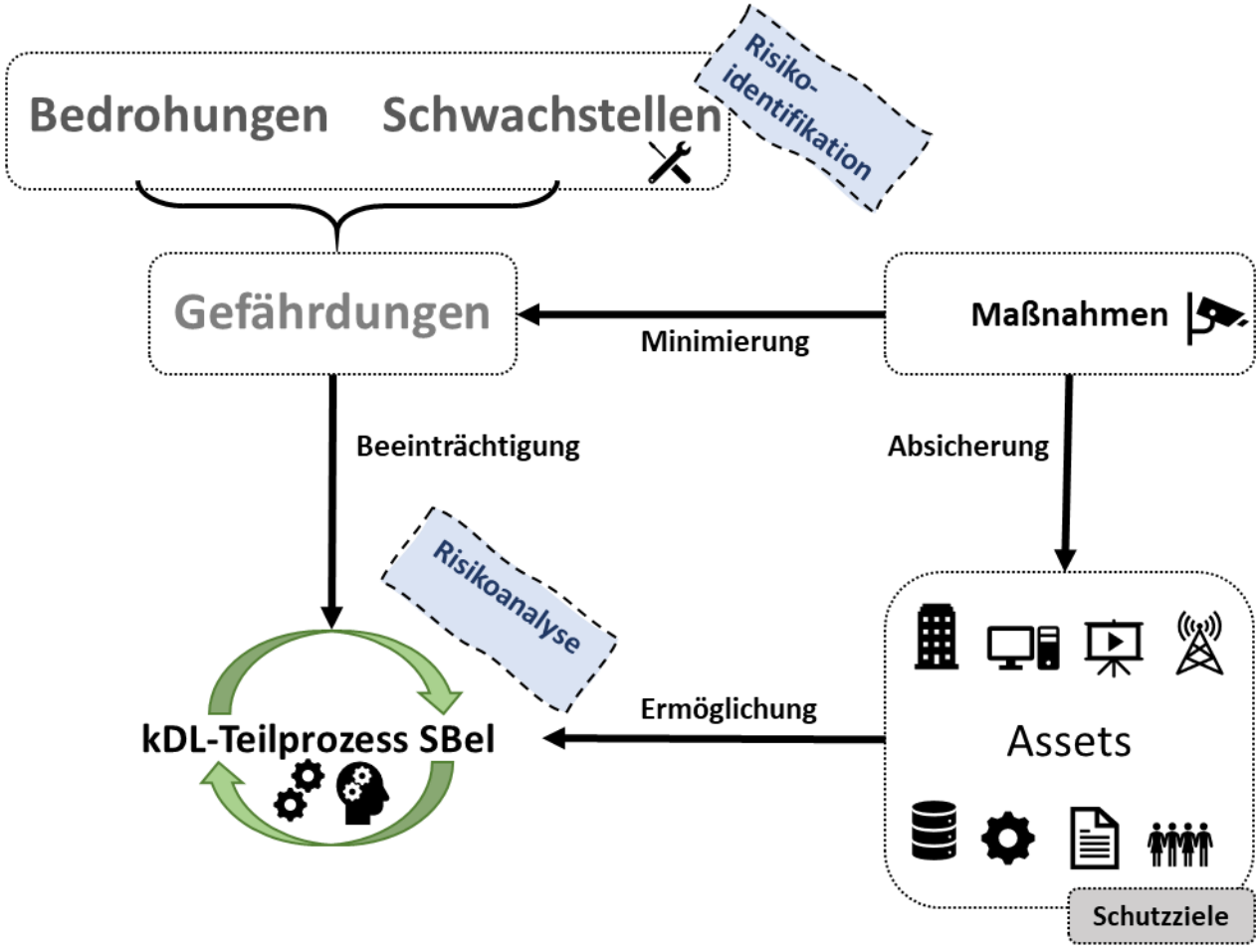

Abbildung 3: Schematische Darstellung des All-Gefahrenansatzes (Icons: www.flaticon.com)

Der All-Gefahrenansatz i.S. des B3S umfasst Bedrohungen und Schwachstellen, die zu Gefährdungen des kDL-Teilprozess SBeL führen können. Zur besseren Verständlichkeit werden im Folgenden wesentliche Begriffe erläutert und ergänzende Verweise aufgeführt.

Der Begriff **Bedrohung** (englisch: threat) im Kontext des B3S definiert einen Einfluss, der zu einer Beeinträchtigung der Vertraulichkeit, Integrität, oder Verfügbarkeit von Informationen oder Prozessen führen kann. Die Auswirkung der Beeinträchtigung kann einen Schaden des Informationsnutzers nach sich ziehen. Bei der Erfassung möglicher Bedrohungen gibt die ISO 27005 Annex C gute Anhaltspunkte. Beispiele für Bedrohungen sind Naturgefahren, menschliche (auch unbeabsichtigte) Handlungen oder technisches Versagen. Zudem sollten identifizierte branchenspezifische Bedrohungen herangezogen werden, durch die ein Schaden entstehen kann.

Der Begriff **Schwachstelle** (englisch: vulnerability) im Kontext des B3S beschreibt einen Fehler oder eine Lücke im Bereich der Sicherheit. Eine Schwachstelle kann die Wirksamkeit einer Bedrohung ermöglichen und damit zu einem Schaden führen. Dabei bezieht sich der Schaden auf Werte wie Vermögen, spezifisches Wissen, Gegenstände oder Gesundheit. Ein Asset kann durch eine Schwachstelle anfällig für eine Bedrohung werden. Die ISO 27005 Annex D listet grundlegende Schwachstellen auf.

Trifft eine Bedrohung auf eine Schwachstelle, so entsteht eine **Gefährdung** (vgl. BSI IT-Grundschutz). Anders ausgedrückt, entsteht erst eine Gefährdung für ein Asset, wenn eine Bedrohung eine vorhandene Schwachstelle nutzt. Gefährdungen im Sinne der Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung - BSI-KritisV) sind Dienstleistungen zur Versorgung der Allgemeinheit in den Sektoren nach den §§ 2 bis 8, deren Ausfall oder Beeinträchtigung zu erheblichen Versorgungsengpässen oder zu Gefährdungen der öffentlichen Sicherheit führen würde. Das BSI führt in dem IT-Grundschutzkatalog verschiedene elementare Gefährdungen auf, die sich negativ auf den kDL-Teilprozess SBeL auswirken und somit beeinträchtigen können.

Risiko ist ein Maß für die Gefährdung, die von einer Bedrohung ausgeht und setzt sich zusammen aus zwei Komponenten: der Wahrscheinlichkeit, mit der das Ereignis eintritt, und der Höhe des Schadens, der als Folge des Ereignisses auftritt.

Mit Hilfe der **Risikoidentifikation** werden Bedrohungen als auch Schwachstellen erfasst (siehe ISO 27005 Annex C & D).

Die **Risikoanalyse** und **-bewertung** prüft die potenziellen Gefährdungen und ihre Auswirkung auf den kDL-Teilprozess SBeL. Dabei werden auch die zu grundliegenden Assets betrachtet.

Abgeleitet von der **Risikobehandlung** werden **angemessene Maßnahmen** ergriffen, die eine Beeinträchtigung der Assets verhindern und die Wirksamkeit von Gefährdungen mindern sollen. Die Umsetzung geeigneter Maßnahmen haben das Ziel den kDL-Teilprozess SBeL abzusichern.

Der B3S empfiehlt die grundsätzliche Erfassung von Bedrohungen und Schwachstellen, um zu den gesamthaften Gefährdungen zu gelangen. Da sich die Gefährdungslagen ständig ändern, ist es empfehlenswert, eine regelmäßige Risikoanalyse durchzuführen. Hierdurch soll die Effektivität der zu ergreifenden Sicherheitsmaßnahmen überprüft werden.

2.2 Benennung der Bedrohungen und Schwachstellen

In der folgenden Tabelle werden die mindestens zu betrachtenden Bedrohungskategorien und Schwachstellen bzw. Gefährdungen hinsichtlich ihrer Relevanz anhand beispielhafter branchenspezifischer Szenarien bewertet.

Diese Bewertung ersetzt nicht die Risikobewertung, die jeder Betreiber im Rahmen der Umsetzung dieses B3S selbst vorzunehmen hat. Wenn im Einzelfall notwendig (oder sinnvoll), müssen durch den Betreiber für den Geltungsbereich des B3S relevante, konkrete Bedrohungen und Schwachstellen bzw. sich daraus ergebende Gefährdungen ausdrücklich benannt und bewertet werden.

Bedrohungskategorien und Schwachstellen bzw. Gefährdungen

Risiko	Branchenspezifische Relevanz
Hacking und Manipulation	Hacking und Manipulation des Leit- / Steuersystems können weitreichende Auswirkungen auf den kDL-Teilprozess SBeL haben, wenn beispielsweise die Steuerbarkeit für längere Zeit nicht mehr gewährleistet ist oder manipulierte Steuerbefehle ausgelöst werden können.
Terroristische Akte	Beispielsweise können physische Angriffe auf Rechenzentrumsstandorte der Leit- / Steuersysteme zu einem Ausfall der Steuerbarkeit und damit zu Auswirkungen auf den kDL-Teilprozess SBeL führen.
Naturgefahren (Naturkatastrophen im Umfeld)	Naturkatastrophen im Bereich der Rechenzentrumsstandorte der Leit- / Steuersysteme können zu einem Ausfall der Steuerbarkeit führen und damit Auswirkungen auf den kDL-Teilprozess SBeL haben.
Identitätsmissbrauch (Phishing, Skimming, Zertifikatsfälschung)	Identitätsmissbrauch, der zu unbefugtem Zugriff auf das Leit- / Steuersystem führt, kann weitreichende Auswirkungen auf den kDL-Teilprozess SBeL haben, wenn beispielsweise die Steuerbarkeit für längere Zeit nicht mehr gewährleistet ist oder manipulierte Steuerbefehle ausgelöst werden können.
Missbrauch (Innentäter)	Ein Missbrauch durch Innentäter, der weitreichenden Zugriff auf das Leit- / Steuersystem hat, kann weitreichende Auswirkungen auf den kDL-Teilprozess SBeL haben, wenn beispielsweise die Steuerbarkeit für längere Zeit nicht mehr gewährleistet ist oder manipulierte Steuerbefehle ausgelöst werden können.

Abhängigkeiten von Dienstleistern und Herstellern (Ausfall externer Dienstleister, unberechtigter Zugriff, versteckte Funktionen in Hard- und Software)	Ein weitreichender Ausfall der Technik der Telekommunikationsdienstleister, die zur Kommunikation mit den dezentralen Anlagen benötigt wird, kann weitreichende Auswirkungen auf den kDL-Teilprozess SBeL haben, wenn hierdurch die Steuerbarkeit für längere Zeit nicht mehr gewährleistet werden kann.
Unbefugter Zugriff	Unbefugter Zugriff auf das Leit- / Steuersystem kann weitreichende Auswirkungen auf den kDL-Teilprozess SBeL haben, wenn beispielsweise die Steuerbarkeit für längere Zeit nicht mehr gewährleistet ist oder manipulierte Steuerbefehle ausgelöst werden können.
Manipulation, Diebstahl, Verlust, Zerstörung von IT oder IT-relevanten Anlagen und Anlagenteilen	Manipulation des Leit- / Steuersystems kann weitreichende Auswirkungen auf den kDL-Teilprozess SBeL haben, wenn beispielsweise die Steuerbarkeit für längere Zeit nicht mehr gewährleistet ist oder manipulierte Steuerbefehle ausgelöst werden können. Diebstahl, Verlust und Zerstörung von wesentlichen Komponenten des Leit- / Steuersystems kann zu einem Verlust der Steuerbarkeit führen.
Schadprogramme	Schadprogramme, die zu gezielten Manipulationen des Leit- / Steuersystems führen, können weitreichende Auswirkungen auf den kDL-Teilprozess SBeL haben, wenn beispielsweise die Steuerbarkeit für längere Zeit nicht mehr gewährleistet ist oder manipulierte Steuerbefehle ausgelöst werden können.
Social Engineering	Durch Social Engineering könnten sich Unbefugte Zugriff auf geschützte Systemschnittstellen verschaffen. Eine Manipulation dieser kann weitreichende Auswirkungen auf den kDL-Teilprozess SBeL haben, wenn beispielsweise die Steuerbarkeit für längere Zeit nicht mehr gewährleistet ist oder manipulierte Steuerbefehle ausgelöst werden können.
Gezielte Störung / Verhinderung von Diensten (DDoS, gezielte Systemabstürze, ...)	Gezielte Störungen der öffentlichen Kommunikationsanbindungen können zu Nicht-Erreichbarkeit des Leit- / Steuersystems für den Betreiber (z.B. Netzbetreiber, Direktvermarkter, usw.) führen.

	Dadurch könnte die planmäßige Steuerbarkeit nicht gewährleistet werden.
Advanced Persistent Threat (APT)	Ein APT Angriff, über den Zugriff auf das zentrale Leit- / Steuersystem erlangt wird, kann weitreichende Auswirkungen auf den kDL-Teilprozess SBeL haben, wenn beispielsweise die Steuerbarkeit für längere Zeit nicht mehr gewährleistet ist oder manipulierte Steuerbefehle ausgelöst werden können.
Beschädigung oder Zerstörung verfahrenstechnischer Komponenten, Ausrüstungen und Systemen	Beschädigung oder Zerstörung des Leit- / Steuersystems kann weitreichende Auswirkungen auf den kDL-Teilprozess SBeL haben, wenn beispielsweise die Steuerbarkeit für längere Zeit nicht mehr gewährleistet ist.
Organisatorische Mängel	Durch organisatorische Mängel kann ein dauerhaft sicherer Betrieb des Aggregators gefährdet werden.
Technische Schwachstellen in Software, Firmware und Hardware	Technische Schwachstellen in Software, Firmware und Hardware können dazu führen, dass sich Unbefugte Zugriff auf das zentrale Leit- / Steuersystem verschaffen. Dies kann weitreichende Auswirkungen auf den kDL-Teilprozess SBeL haben, wenn beispielsweise die Steuerbarkeit für längere Zeit nicht mehr gewährleistet ist oder manipulierte Steuerbefehle ausgelöst werden können.
Technisches Versagen von IT-Systemen, Anwendungen oder Netzen (sowie Verlust von gespeicherten Daten)	Technisches Versagen von IT-Systemen, Anwendungen oder Netzen kann bei fehlender Redundanz weitreichende Auswirkungen auf den kDL-Teilprozess SBeL haben, wenn beispielsweise die Steuerbarkeit für längere Zeit nicht mehr gewährleistet ist.
Menschliche Fehlhandlungen, menschliches Versagen	Menschliche Fehlhandlungen oder menschliches Versagen können z.B. in Form von Fehlkonfigurationen des zentralen Leit-/ Steuersystems zu Systemausfällen führen, und somit Auswirkungen auf den kDL-Teilprozess SBeL haben, wenn beispielsweise die Steuerbarkeit für längere Zeit nicht mehr gewährleistet ist.
Infrastrukturelle Mängel (baulich, Versorgung mit Strom etc.)	Infrastrukturelle Mängel, die zu einem Ausfall oder Beeinträchtigung des zentralen Leit- / Steuersystems führen, können weitreichende Auswirkungen

	auf den kDL-Teilprozess SBeL haben, wenn beispielsweise die Steuerbarkeit für längere Zeit nicht mehr gewährleistet ist.
Verwendung ungeeigneter Netze/ Kommunikationsverbindungen, sonstige Schwächen in der Kommunikationsarchitektur	Die Verwendung ungeeigneter Netze kann zu Einschränkungen der Verfügbarkeit führen, beispielsweise durch zu geringe Bandbreite oder Verfügbarkeit der Kommunikationsverbindung.
Verkopplung von Diensten (Beeinträchtigung eines Dienstes durch Störung anderer Dienste)	Störungen in anderen Diensten, z.B. öffentlichen Telekommunikationsnetzen oder der örtlichen Stromversorgung können zu Einschränkungen der Verfügbarkeit führen.
Manipulation der Datenübertragung über ungesicherte Fernwirkprotokolle	Manipulationen von Datenübertragungen zu einer Vielzahl von dezentralen Anlagen können weitreichende Auswirkungen auf den kDL-Teilprozess SBeL haben, wenn beispielsweise manipulierte Steuerbefehle ausgelöst werden.

3 RISIKOBEHANDLUNG (Risikomanagement)

3.1 Geeignete Behandlung aller für den kDL-Teilprozess relevanten Risiken

Im Rahmen des Risikomanagements des ISMS muss der Aggregator die für den kDL-Teilprozess SBeL relevanten Risiken hinreichend behandeln. Die Risikobehandlung umfasst dabei eine Risikoreduktion oder eine Risikovermeidung, die Möglichkeiten zur Risikoakzeptanz werden durch diesen B3S explizit eingeschränkt (siehe Abschnitt 3.2).

Im ersten Schritt müssen hierfür die Gefährdungskategorien gemäß Abschnitt 2.2 bewertet werden. Im zweiten Schritt muss der daraufhin ermittelte Handlungsbedarf umgesetzt werden.

Dabei sollen vorhandene Rückfallpositionen und -mechanismen seitens der Betreiber in die Risikoanalyse einfließen. Beispiele für solche häufig in der Branche vorhandene Rückfallpositionen sind:

- Alternative Kommunikationswege (z.B. Telefon, Fax) zu relevanten Stakeholdern bzw. zu Netzbetreibern, im Falle der Erbringung von Regelleistung,
- Redundanzen bei z.B. Kommunikationsmittel, Systemlandschaften oder Arbeitsabläufen,
- Autarkie der Erzeugungs- oder Verbrauchsanlagen, d.h. die Erzeugungs- oder Verbrauchsanlagen produzieren bzw. verbrauchen bei einem Ausbleiben von neuen

Steuersignalen z.B. aufgrund eines Ausfalls des Aggregators im Regelfall auf gleichem Niveau weiter.

Dazu müssen, basierend auf einer Bewertung der Risiken, die vorhandenen Maßnahmen mit den vorgeschlagenen Maßnahmen des Anhangs A der ISO/IEC 27001 und der ISO/IEC 27019 abgeglichen werden, und

- **die Formulierung des jeweiligen Handlungsbedarfs,**
- **die Umsetzung des formulierten Handlungsbedarfs und**
- **die regelmäßige Überprüfung dieses Analyse- und Planungsprozesses**

im Rahmen des Informationssicherheitsmanagements erfolgen.

Für die Identifizierung der für den kDL-Teilprozess SBeL relevanten Risiken müssen mindestens die Anforderungen gemäß 6.1.2 Information Security Risk Assessment ISO/IEC 27001:2013 berücksichtigt werden.

Der Risikobehandlungsprozess muss mindestens gemäß 6.1.3 Information Security Risk Treatment und 6.1.2 ISO/IEC 27001:2013 sowie zusätzlich entweder gemäß der Abschnitte 9.1 - 9.5 ISO/IEC 27005:2013 oder Abschnitt 5.5 ISO/IEC 31000 erfolgen.

3.2 Beschränkung der Behandlungsalternativen für Risiken

Im Rahmen des ISMS müssen für das Risikomanagement explizit Grenzen bei der Auswahl der Behandlungsalternativen im Sinne des BSIG festgelegt werden. Der hier vorliegende B3S schränkt hierbei explizit Optionen gegenüber allgemeinen Risikomanagementansätzen ein. Eingeschränkt wird insbesondere eine dauerhafte Akzeptanz von relevanten Risiken für informationstechnische Systeme, Komponenten oder Prozesse des kDL-Teilprozesses SBeL auch in Kombination mit Risikoversicherungen. Dies ist nicht zulässig, unter der Maßgabe, dass der Aufwand in einem angemessenen Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung des kDL-Teilprozesses SBeL und ihrer jeweiligen Auswirkungen auf die kritische Dienstleistung Stromversorgung steht.

Die volle Verantwortung für eine geeignete Risikobehandlung verbleibt stets beim Betreiber des Aggregators. Dieses gilt auch bei der Einbindung von Drittdienstleistern (siehe hierzu auch Abschnitt 1.2 „Geltungsbereich umfasst auch extern erbrachte Leistungen“).

3.3 Berücksichtigung von Abhängigkeiten bei der Risikoanalyse

In der Risikoanalyse müssen die Abhängigkeiten der eigenen IT-Systeme von IT-Systemen Dritter, z. B. Auswirkungen von Störungen verbundener IT-Systeme anderer Betreiber / Dritter auf die eigenen IT-Systeme berücksichtigt werden, die für die Erbringung des kDL-Teilprozesses SBeL relevant sind. Hierzu sind A 15.1 und A 15.2 der ISO/IEC 27001:2013 umzusetzen.

3.4 Änderung der allgemeinen und branchenspezifischen Gefährdungslage

Es ist eine kontinuierliche Beobachtung der Gefährdungslage erforderlich. Die Ergebnisse dieser Beobachtungen müssen bei einer anlassbezogenen, mindestens jedoch einmal jährlich stattfindenden Überprüfung der Risikoanalyse berücksichtigt werden und die Risikoanalyse bei Bedarf aktualisiert werden. Dabei müssen sowohl Änderungen der allgemeinen als auch der branchenspezifischen Gefährdungslage, berücksichtigt werden (gemäß Abschnitt 8.2 ISO/IEC 27001:2013). Dieses beinhaltet insbesondere die Betrachtung von:

- **allgemeine Bedrohungen (neu hinzugekommene Typen von Angreifern und Angriffen, intensivere Aktivität oder verbesserte Expertise / Ressourcen von Angreifern sowie Neuausrichtung von Angreifern),**
- **bekannt gewordene neue Schwachstellen,**
- **Änderungen der Gefährdungslage durch Veränderungen an der informationstechnischen Systemarchitektur,**
- **anderweitige Änderungen der Exposition von Informations- und Kommunikationssystemen, die für die Erbringung des kDL-Teilprozesses SBeL relevant sind,**
- **Änderungen an Betriebsabläufen und Geschäftsprozessen sowie neuen Produkte, soweit diese für die Erbringung des kDL-Teilprozesses SBeL relevant sind.**

4 ANGEMESSENE VORKEHRUNGEN (MASSNAHMEN)

4.1 Angemessenheit der Maßnahmen

Der Betreiber muss die für den kDL-Teilprozess SBeL ermittelten Risiken hinsichtlich der informationstechnischen Systeme, Komponenten oder Prozesse identifizieren und bewerten, so dass die Anforderungen an die Erbringung der kritischen Dienstleistung erfüllt werden können.

Im Sinne dieses B3S Steuerung / Bündelung elektrischer Leistung sind organisatorische und technische Vorkehrungen gemäß § 8a Abs. 1 Satz 3 BSIG angemessen, wenn der dafür erforderliche Aufwand nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung der betroffenen Kritischen Infrastruktur für den kDL-Teilprozess SBeL steht.

4.2 Eignung von Maßnahmen

Der Betreiber ist verpflichtet, verfahrensseitig gemäß Abschnitt 6.1.1 d) und e) der ISO/IEC 27001:2013 sicherzustellen, dass die zu ergreifenden Maßnahmen geeignet sind, d.h., dass sie wirken. Mittels einer maßnahmenspezifischen Wirksamkeitsbewertung, die in ausreichenden Maß den beabsichtigten Zweck mit dem erzielten Ergebnis vergleicht, muss der Betreiber nachweisen, dass das Risiko und unerwünschte Nebeneffekte minimiert wurden. Das ISMS wählt basierend auf Abschnitt 6.1.3 a) und b) ISO/IEC 27002:2013 dafür geeignete Maßnahmen unter Berücksichtigung der ISO/IEC 27002:2013 und ISO/IEC 27019:2017 aus.

5 ABZUDECKENDE THEMEN

5.1 Abdeckung relevanter Themen

Dieser B3S definiert Anforderungen zu Abdeckung der nachfolgenden Themenfelder:

- **Informationssicherheitsmanagementsystem (ISMS)**
- **Risikoanalysemethoden**
- **Continuity und Notfall-Management**
- **Asset Management**
- **Bauliche / physische Sicherheit**
- **Personelle und organisatorische Sicherheit**
- **Branchenspezifische Technik**
- **Vorfallserkennung und -bearbeitung**
- **Überprüfung im laufenden Betrieb**
- **Externe Informationsversorgung und Unterstützung**
- **Lieferanten, Dienstleister und Dritte**
- **Technische Informationssicherheit**

Die Notwendigkeit, bestimmte Controls zu implementieren, ergibt sich dabei aus dem Ergebnis der Risikoanalyse. Die im Folgenden aufgeführten Controls sind nicht als abschließende Liste zu betrachten. Sie sollen dem Betreiber bei der Anwendung des B3S vielmehr die im Rahmen des Risikomanagements gemäß ISO/IEC 27001, 6.1.3 mindestens zu berücksichtigenden Controls aufzeigen. Diese sind bei Bedarf zu erweitern.

Ergänzend werden zu verschiedenen relevanten Themen Umsetzungshinweise aus dem BDEW/OE Whitepaper V2.0 gegeben, die bei der Ausgestaltung der Maßnahmen unterstützen können.

5.2 Informationssicherheitsmanagementsystem (ISMS)

Die Anforderungen an das Informationssicherheitsmanagementsystem sind bereits in Abschnitt 1.2 aufgeführt.

5.3 Risikoanalysemethoden

Die Anforderungen an Risikoanalysemethoden sind bereits in Kapitel 3 aufgeführt.

5.4 Continuity und Notfall-Management

Der Betreiber muss im Rahmen eines Continuity- und Notfallmanagements gewährleisten, dass der kDL-Teilprozess SBeL auch bei IT-Störungen und Angriffen so weit wie möglich aufrechterhalten wird. Hierzu sind auch entsprechende Tests und Übungen vorzusehen.

Hierzu sind mindestens die folgenden Controls und Umsetzungsempfehlungen der ISO/IEC 27001 und 27019 gemäß dem Ergebnis der Risikoanalyse nach Abschnitt 3.1 zu implementieren:

ISO/IEC 27001

- A.17.1.1 Planning information security continuity
- A.17.1.2 Implementing information security continuity
- A.17.1.3 Verify, review and evaluate information security continuity
- A.17.2.1 Availibility of information processing facilities

ISO/IEC 27019

- 17.2.1 Availability of information processing facilities
- 17.2.2 ENR – Emergency communication

Umsetzungshinweise, die bei der Ausgestaltung der Maßnahmen unterstützen können:
BDEW/OE Whitepaper:
4.8.1 Backup: Konzept, Verfahren, Dokumentation, Tests
4.8.2 Notfallkonzeption und Wiederanlaufplanung

5.5 Asset Management

Das ISMS muss eine geeignete Verfahrensweise für die Identifikation, Klassifizierung und Inventarisierung der maßgeblichen informationstechnischen Prozesse, Systeme und Komponenten sowie deren zugeordneten Verantwortlichen definieren.

Hierzu sind mindestens die folgenden Controls und Umsetzungsempfehlungen der ISO/IEC 27001 und 27019 gemäß dem Ergebnis der Risikoanalyse nach Abschnitt 3.1 zu implementieren:

ISO/IEC 27001

- A.8.1.1 Inventory of assets
- A.8.1.2 Ownership of assets
- A.8.1.3 Acceptable use of assets

A.8.1.4 Return of assets

A.8.2.1 Classification of information

A.8.2.2 Labelling of information

A.8.2.3 Handling of assets ISO/IEC 27019

Umsetzungshinweise, die bei der Ausgestaltung der Maßnahmen unterstützen können: BDEW/OE Whitepaper: 4.4.3 Dokumentation der Netzwerkstruktur und -konfiguration

5.6 Bauliche / physische Sicherheit

Durch bauliche und physische Sicherheit wird der Zutritt zu - und damit Zugriff auf - sensible Bereiche des Unternehmens für unberechtigte Personen verhindert.

Hierzu sind mindestens die folgenden Controls und Umsetzungsempfehlungen der ISO/IEC 27001 und 27019 gemäß dem Ergebnis der Risikoanalyse nach Abschnitt 3.1 zu implementieren:

ISO/IEC 27001

A.11.1.1 Physical security perimeter

A.11.1.2 Physical entry controls

A.11.1.3 Securing offices, rooms and facilities

A.11.1.4 Protecting against external and enviromental threats

A.11.1.5 Working in secure areas

A.11.1.6 Delivery and loading areas

A.11.2.1 Equipment and siting protection

A.11.2.2 Supporting utilities

A.11.2.3 Cabeling security

A.11.2.4 Equipment maintenance

A.11.2.5 Removal of Assets

A.11.2.6 Security of equipment and assets off-premises

A.11.2.7 Secure disposal or reuse of equipment

A.11.2.8 Unattended user equipment

A.11.2.9 Clear desk and clear screen policy

ISO/IEC 27019

- 11.1.1 Physical security perimeter
- 11.1.2 Physical entry controls
- 11.1.7 ENR – Securing control centres
- 11.1.8 ENR – Securing equipment rooms
- 11.1.9 ENR – Securing peripheral sites
- 11.2.1 Equipment siting and protection
- 11.2.2 Supporting utilities
- 11.2.3 Cabling security
- 11.2.9 Clear desk and clear screen policy
- 11.3.1 ENR – Equipment sited on the premises of other energy utility organizations
- 11.3.2 ENR – Equipment sited on customer's premises
- 11.3.3 ENR – Interconnected control and communication systems

Umsetzungshinweise, die bei der Ausgestaltung der Maßnahmen unterstützen können: BDEW/OE Whitepaper: 4.1.10 Anforderungen an die Dokumentation

5.7 Personelle und organisatorische Sicherheit

Personelle und organisatorische Sicherheit trägt insbesondere zum Sabotageschutz im Unternehmen bei und soll somit verhindern, dass unberechtigte Personen Zugriff auf oder Zutritt zu sensiblen Bereichen des Unternehmens erlangen können.

Hierzu sind mindestens die folgenden Controls und Umsetzungsempfehlungen der ISO/IEC 27001 und 27019 gemäß dem Ergebnis der Risikoanalyse nach Abschnitt 3.1 zu implementieren:

ISO/IEC 27001

- A.6.1.1 Information security roles and responsibilities
- A.7.1.1 Screening
- A.7.1.2 Terms and conditions of employment
- A.7.2.1 Management responsibilities
- A.7.2.2 Information security awareness, education and training
- A.7.2.3 Disciplinary process

A.7.3.1 Termination or change of employment resposibilities

ISO/IEC 27019

6.1.1 Information security roles and responsibilities

6.1.7 ENR – Addressing security when dealing with customers

7.1.1 Screening

7.1.2 Terms and conditions of employment

7.2.2 Information security awareness, education and training

5.8 Branchenspezifische Technik

Bei Aggregatoren werden zur Datenkommunikation häufig branchenspezifische Fernwirk-/Industrieprotokolle eingesetzt. Beispielhaft werden folgend einige branchenspezifische, häufig anzutreffende und relevante Schnittstellen aufgelistet. Gemäß dem Ergebnis der Risikoanalyse nach Abschnitt 3.1 müssen hier gegebenenfalls weitere Maßnahmen umgesetzt werden, damit das Sicherheitsniveau dem Stand der Technik entspricht.

Bei den folgenden Protokollen ist die sicherere Kommunikation durch die unten genannten geeigneten Maßnahmen umzusetzen, sofern entsprechender Schutzbedarf im Sinne dieses B3S besteht. Diese Protokolle bieten dabei von sich aus keinerlei Verschlüsselung, sind nicht gegen Manipulationen geschützt und unterstützen keine Authentifizierung oder Autorisierung.

- **IEC 60870-5-104**
- **Modbus-TCP**

Bei den folgenden Protokollen, die von sich aus lediglich keine Verschlüsselung unterstützen und keinen Schutz vor Manipulation bieten, jedoch eine Authentifizierung, ist die sichere Kommunikation durch die unten beschriebenen geeigneten Maßnahmen umzusetzen, sofern entsprechender Schutzbedarf im Sinne dieses B3S besteht:

- **OPC XML-DA**
- **IEC 61400-25**

Um die Besonderheiten dieser branchenspezifischen Technik zu berücksichtigen, sind die folgenden branchenspezifischen Controls der ISO/IEC 27019 gemäß dem Ergebnis der Risikoanalyse nach Abschnitt 3.1 zu implementieren:

ISO/IEC 27019

13.1.4 ENR – Securing process control data communication

13.1.5 ENR – Logical connection of external process control systems

Umsetzungshinweise, die bei der Ausgestaltung der Maßnahmen unterstützen können:

BDEW/OE Whitepaper:

- 4.1.5 Verschlüsselung vertraulicher Daten
- 4.1.6 Kryptographische Verfahren
- 4.4.1 Eingesetzte Protokolle und Technologien
- 4.4.2 Sichere Netzwerkstruktur
- 4.4.3 Dokumentation der Netzwerkstruktur und -konfiguration

5.9 Vorfallserkennung und –bearbeitung

Durch Maßnahmen zur Vorfallserkennung sollen IT-Vorfälle, Störungen und Angriffe zeitnah detektiert und behandelt werden können.

Hierzu sind mindestens die folgenden Controls der ISO/IEC 27001 und 27019 gemäß dem Ergebnis der Risikoanalyse nach Abschnitt 3.1 zu implementieren:

ISO/IEC 27001

- A.15.2.1 Monitoring and review of supplier services
- A.16.1.1 Responsibilities and procedures
- A.16.1.2 Reporting information security events
- A.16.1.3 Reporting information security weaknesses
- A.16.1.4 Assessment of and decision on information security events
- A.16.1.5 Response to information security incidents
- A.16.1.6 Learning from information security incidents
- A.16.1.7 Collection of evidence

ISO/IEC 27019

- 16.1.5 Response to information security incidents

Hinsichtlich der Umsetzung des Controls A.16.1.7 „Collection of Evidence“ liegt der Schwerpunkt dabei im Sinne dieses B3S auf der Sicherung von Beweisen zum Zwecke eines Erkenntnisgewinns, sowie der Verbesserung des Informationssicherheitsmanagements.

Umsetzungshinweise, die bei der Ausgestaltung der Maßnahmen unterstützen können:

BDEW/OE Whitepaper:

- 4.1.10 Anforderungen an die Dokumentation
- 4.5.6 Logging

5.10 Überprüfung im laufenden Betrieb

Durch Maßnahmen zur Überprüfung sollte die Effektivität der ergriffenen Maßnahmen regelmäßig durch den Betreiber überprüft werden.

Hierzu sind mindestens die folgenden Controls und Umsetzungsempfehlungen der ISO/IEC 27001 und 27019 gemäß dem Ergebnis der Risikoanalyse nach Abschnitt 3.1 zu implementieren:

ISO/IEC 27001

- A.12.4.1 Event-Logging
- A.12.4.2 Protection of Log Information
- A.12.4.3 Administrator and Operator Logs
- A.12.7. Information System Audit Considerations
- A.15.2.1 Monitoring and review of supplier services
- A.18.2.1 Independent Review of Information Security
- A.18.2.2 Compliance with security policies and standards
- A.18.2.3 Technical Compliance Review

ISO/IEC 27019

- 12.4.1 Event Logging
- 18.2.3 Technical Compliance Review

Der Betreiber muss das ISMS sowie die im ISMS aufgetretenen Vorfälle und die dazugehörigen Behandlungspläne zusätzlich gemäß ISO/IEC 27001 9.2 „Internal Audit“ regelmäßig durch interne Audits überprüfen.

5.11 Externe Informationsversorgung und Unterstützung

Zur Aufrechterhaltung und stetigen Verbesserung des Sicherheitsniveaus im Allgemeinen wie auch zur Berücksichtigung aktueller Entwicklungen der für den Betreiber relevanten IT-Sicherheitslage, muss im ISMS eine geeignete Verfahrensweise zur Beschaffung und Verarbeitung von externen und internen sicherheitsrelevanten Informationen (siehe auch Abschnitt 3.4 und 3.5) festgelegt sein. Hierzu gehört auch die Registrierung einer Kontaktstelle gemäß § 8b Absatz 3 BSIG für die Betreiber, damit der Erhalt von Informationen vom BSI gemäß § 8b Absatz 2 Nummer 4 BSIG zur Übermittlung von Informationen durch das BSI gesichert ist.

Zusätzlich sind die folgenden Controls und Umsetzungsempfehlungen der ISO/IEC 27001 und 27019 gemäß dem Ergebnis der Risikoanalyse nach Abschnitt 3.1 zu implementieren:

ISO/IEC 27001

A.6.1.3 Contact with authorities

A.6.1.4 Contact with special interest groups

ISO/IEC 27019

6.1.3 Contact with authorities

6.1.4 Contact with special interest groups

5.12 Lieferanten, Dienstleister und Dritte

Der Betreiber muss geeignete Maßnahmen treffen, um die Einhaltung der Sicherheitsanforderungen durch Lieferanten, Dienstleister und Dritte zu gewährleisten.

Hierzu sind die folgenden Controls und Umsetzungsempfehlungen der ISO/IEC 27001 und 27019 gemäß dem Ergebnis der Risikoanalyse nach Abschnitt 3.1 zu implementieren:

ISO/IEC 27001

A.15.1.1 Information security policy for supplier relationships

A.15.1.2 Addressing security within supplier agreements

A.15.1.3 Information and communication technology supply chain

A.15.2.1 Monitoring and review of supplier services

A.15.2.2 Managing changes to supplier services

ISO/IEC 27019

6.1.6 ENR – Identification of risks related to external parties

6.1.7 ENR – Addressing security when dealing with customers

15.1.2 Addressing security within supplier agreements

Als zusätzliche Hilfestellung zur Umsetzung der vorgenannten Controls können dabei die UP KRITIS *„Best-Practice-Empfehlungen für Anforderungen an Lieferanten zur Gewährleistung der Informationssicherheit in kritischen Infrastrukturen“* sowie das BDEW/OE Whitepaper verwendet werden.

5.13 Technische Informationssicherheit

Zu den in Anhang A in Kapitel 8 aufgelisteten Themen müssen Maßnahmen zur technischen Informationssicherheit identifiziert und umgesetzt werden, wo dies nach dem Ergebnis der Risikoanalyse für die Gewährleistung der Erbringung des kDL-Teilprozess SBeL notwendig ist.

6 NACHWEISBARKEIT DER UMSETZUNG

Der Nachweis erfolgt durch eine prüfende Stelle, welche die fachlichen und organisatorischen Anforderungen der ISO/IEC 27006:2015 „Requirements for bodies providing audit and certification of information security management systems“ erfüllt.

Die ISO/IEC 27006 ist aus dem Leitfaden EA-7/03 der European Accreditation Foundation hervorgegangen. Sie basiert auf der DIN EN ISO/IEC 17021 („Konformitätsbewertung - Anforderungen an Stellen, die Managementsysteme auditieren und zertifizieren“) und ergänzt diese um die ISMS-spezifischen Anforderungen.

Des Weiteren sind die Vorgaben der „Orientierungshilfe zu Nachweisen gemäß § 8a (3) BSIG“ des BSI in der aktuellen Fassung maßgeblich.

Bei Erscheinen neuer Normversionen im Rahmen der Nachweiserbringung gilt eine Übergangsfrist von 1 Jahr. Innerhalb dieser Übergangsfrist können auch die entsprechenden Vorgängerversionen verwendet werden.

7 Literaturverzeichnis

BDEW/OE Whitepaper „Anforderungen an sichere Steuerungs- und Telekommunikationssysteme“	Bundesverband der Energie- und Wasserwirtschaft, Oesterreichs E-Wirtschaft Überarbeitete Version 2.0 05/2018
BDEW-Energie-Info „IT-Sicherheit: Anforderungen bei der Dienstleister- und Herstellerselbstauskunft"	Bundesverband der Energie- und Wasserwirtschaft Version vom 16. Juni 2014
ISO/IEC 27000:2020-06 Informationstechnik - Sicherheitsverfahren – Informationssicherheitsmanagementsysteme - Überblick und Terminologie (ISO/IEC 27000:2018); Deutsche Fassung EN ISO/IEC 27000:202	ISO - International Organization for Standardization IEC - International Electrotechnical Commission Ausgabe 2020-06
ISO/IEC 27001:2013 Information security management systems - Requirements	ISO - International Organization for Standardization IEC - International Electrotechnical Commission 2nd Edition, 2013-10-01
ISO/IEC 27002:2013 Code of practice for information security controls	ISO - International Organization for Standardization IEC - International Electrotechnical Commission 2nd Edition, 2013-10-01
ISO/IEC 27006:2015 Requirements for bodies providing audit and certification of information security management systems	ISO - International Organization for Standardization IEC - International Electrotechnical Commission 3rd Edition, 2015-10-01

ISO/IEC 27019:2017 Information security controls for the energy utility industry	ISO - International Organization for Standardization IEC - International Electrotechnical Commission 1st Edition, 2017-10
IT-Sicherheitskatalog gemäß § 11 Absatz 1a Energiewirtschaftsgesetz	Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen, Bonn August 2015
Mindestanforderungen an die Informationstechnik des Anbieters für die Erbringung von Regelleistung	50Hertz Transmission GmbH (Berlin) Amprion GmbH (Pulheim) TenneT TSO GmbH (Bayreuth) TransnetBW GmbH (Stuttgart) Version 2.0 vom 26. Oktober 2018
Orientierungshilfe zu Nachweisen gemäß § 8a (3) BSIG	Bundesamt für Sicherheit in der Informationstechnik Version 1.1 vom 28.08.2020
Orientierungshilfe zu Inhalten und Anforderungen an branchenspezifische Sicherheitsstandards (B3S) gemäß § 8a (2) BSIG	Bundesamt für Sicherheit in der Informationstechnik Version 1.0 vom 01.12.2017

Ansprechpartner

Yassin Bendjebbour
Abteilung Betriebswirtschaft,
Steuern und Digitalisierung
Telefon: +49 30 300199-1526
yassin.bendjebbour@bdew.de

8 Anhang A – Maßnahmen Technische Informationssicherheit

Die folgenden Tabellen führen die gemäß der Orientierungshilfe zu Inhalten und Anforderungen an branchenspezifische Sicherheitsstandards (B3S) gemäß § 8a (2) BSIG des BSI im Rahmen des ISMS mindestens zu behandelnden Themen der Technischen Informationssicherheit auf. Die Referenz ist ein Verweis auf die Nummerierung im BSI-Dokument.

Absicherung von Netzübergängen				
Referenz	**Maßnahme**	**Anforderung**	**Norm-Kapitel**	**Beispiele und Hinweise**
A 3.1.1	Inventarisierung aller Netzzugänge	Alle Zugänge zu Netzwerken zur Messung, Überwachung, Steuerung und Regelung des kDL-Teilprozesses SBeL müssen erfasst sein.	ISO/IEC 27001 A.13.1.1 ISO/IEC 27019 11.3.3	• Siehe hierzu auch BDEW/OE Whitepaper, 4.4.3 Dokumentation der Netzwerkstruktur und -konfiguration • Die Inventarisierung sollte auch alle Zugänge und Übergänge von und zu Dritten umfassen
A 3.1.2	Netztrennung und Segmentierung, besonders im ICS-Umfeld	Die Netzwerke zur Messung, Überwachung, Steuerung und Regelung des kDL-Teilprozesses SBeL müssen von weiteren Netzwerken, z.B. zur sonstigen Bürokommunikation, logisch separiert werden.	ISO/IEC 27001 A.13.1.3 ISO/IEC 27019 13.1.3 ISO/IEC 27019 13.1.4 ENR ISO/IEC 27019 13.1.5 ENR	• Siehe hierzu auch BDEW/OE Whitepaper, 4.4.2 Sichere Netzwerkstruktur
A 3.1.3	Absicherung der Fernzugriffe, Remote Access	Alle Fernzugriffsmöglichkeiten zu Netzwerken zur Messung, Überwachung, Steuerung und Regelung des kDL-Teilprozesses SBeL müssen nach Stand der Technik gesichert sein.	ISO/IEC 27001 A.6.2.2 ISO/IEC 27019 6.2.2 ISO/IEC 27001 A.13.1.3 ISO/IEC 27019 13.1.3	• Siehe hierzu auch BDEW/OE Whitepaper, 4.4.4 Sichere Fern-Zugänge

A 3.1.4	Sicheres Sicherheitsgateway, Firewall	Die Anbindung von Netzwerken zur Messung, Überwachung, Steuerung und Regelung des kDL-Teilprozesses SBeL an weitere Netzwerke muss über eine Firewall mit einem restriktiven Regelsatz erfolgen. Siehe auch A 3.1.2	ISO/IEC 27001 A.13.1.2 ISO/IEC 27001 A.13.1.3 ISO/IEC 27019 13.1.3 ISO/IEC 27019 13.1.5 ENR	• Siehe hierzu auch BDEW/OE Whitepaper, 4.4.2 Sichere Netzwerkstruktur
A 3.1.5	Härtung und sichere Basiskonfigurationen	Alle Netzwerkkomponenten von Netzwerken zur Messung, Überwachung, Steuerung und Regelung des kDL-Teilprozesses SBeL und von Übergängen zu diesen Netzwerken müssen nach aktuellen Empfehlungen gehärtet, d.h. mit einer sicheren Basiskonfiguration versehen sein.	ISO/IEC 27001 A.13.1.1 ISO/IEC 27019 13.1.1 ISO/IEC 27001 A.13.1.3 ISO/IEC 27019 13.1.3	• Siehe hierzu auch BDEW/OE Whitepaper, 4.3.1 Grundsicherung und Systemhärtung
A 3.1.6	Schnittstellenkontrolle, Intrusion Detection/Prevention (IDS, IPS)	Alle Netzübergängen und Schnittstellen zu Netzwerken zur Messung, Überwachung, Steuerung und Regelung des kDL-Teilprozesses SBeL müssen überwacht werden.	ISO/IEC 27001 A.13.1.2 ISO/IEC 27019 13.15. ENR	• Eine Überwachung kann beispielsweise durch die Implementierung eines Network Security Monitorings, den Einsatz einer Security Information and Event Management (SIEM)-Lösung, durch Intrusion Detection / Prevention Systeme (IDS/IPS) oder anderweitiges Monitoring erfolgen. • Bei der Nutzung von Intrusion Prevention Systemen muss insbesondere die Verfügbarkeitsproblematik der für Messung, Überwachung, Steuerung und Regelung

				notwendigen Kommunikation berücksichtigt werden. • Ebenfalls zu prüfen ist, ob durch den Einsatz von IDS/IPS-Systemen ohne das Aufbrechen von bereits verschlüsseltem Datenverkehr ein weiterer Informationsgewinn möglich ist oder mit dem Aufbrechen von verschlüsseltem Datenverkehr verbundene Risiken (Integrität, Authentizität) vom Anwender des B3S hinreichend betrachtet und abgewogen wurden. • Auch eine Überwachung anhand der Auslastung und der Metadaten, um Anomalien zu erkennen, kann eine Möglichkeit der Überwachung sein, ohne den verschlüsselten Datenverkehr aufzubrechen.
A 3.1.7	Absicherung mobiler Netzzugänge, mobile Sicherheit, Telearbeit, ggf. BYOD	Alle für mobile Netzzugänge und Telearbeit genutzten Netzübergangskomponenten sowie die zugehörigen Endgeräte müssen nach Stand der Technik gesichert sein.	ISO/IEC 27001 A.6.2.1 ISO/IEC 27019 6.2.1 ISO/IEC 27001 A.6.2.2 ISO/IEC 27019 6.2.2	• Siehe hierzu auch BDEW/OE Whitepaper, 4.4.4 Sichere Fern-Zugänge
A 3.1.8	DDoS-Mitigation	Über das öffentliche Internet zugängliche Netzübergänge zur Messung, Überwachung, Steuerung und Regelung des kDL-Teilprozesses SBeL	ISO/IEC 27001 A.13.2.3 ISO/IEC 27001 A.17.2.1 ISO/IEC 27019 17.2.1	• Es sollten Ersatzwege vorgesehen werden, über die im Falle eines DDoS-Angriffs auf den Primärweg die wesentlichen Funktionen zur

		müssen gegen DDoS-Angriffe geschützt werden.	ISO/I§C 27019 17.2.2 ENR	Messung, Überwachung, Steuerung und Regelung im notwendigen Mindestumfang aufrechterhalten werden können • Für Ersatzwege sollten im Hinblick auf Vertraulichkeit und Authentizität vergleichbare Sicherheitsmaßnahmen wie für den Primärweg umgesetzt werden.
A 3.1.9	Network Access Control (NAC)	Netzwerke zur Messung, Überwachung, Steuerung und Regelung des kDL-Teilprozesses SBeL müssen über eine Netzzugangskontrolle vor unberechtigtem Zugriff geschützt werden.	ISO/IEC 27001 A.9.1.2 ISO/IEC 27019 9.1.2 ISO/IEC 27001 A.13.1.1 ISO/IEC 27019 13.1.1	
A 3.1.10	Router, VPN-Gateway	Siehe A 3.1.5		• ISO/IEC 27033-5 gibt Empfehlungen und Hinweise zur Kommunikation zwischen Netzwerken mithilfe von virtuellen privaten Netzwerken (VPNs)

Sichere Interaktion im Internet				
Referenz	**Maßnahme**	**Anforderung**	**Norm-Kapitel**	**Beispiele und Hinweise**
A 3.2.1	Browser-Virtualisierung, Exploit Protection	Ein Browserzugriff auf Internet-Ressourcen darf aus Netzwerken zur Messung, Überwachung, Steuerung und Regelung des kDL-Teilprozesses	ISO/IEC 27001 A.12.2.1 ISO/IEC 27019 12.2.1	• Die Browser-Virtualisierung kann beispielsweise durch Sandboxing realisiert werden

		SBeL nur unter Nutzung einer Browser-Virtualisierung bzw. Exploit-Protection erfolgen.		
A 3.2.2	Web-Filter	Ein Zugriff auf Internet-Ressourcen darf aus Netzwerken zur Messung, Überwachung, Steuerung und Regelung des kDL-Teilprozesses SBeL nur über einen Sicherheits-Proxy erfolgen.	ISO/IEC 27001 A.13.1.3 ISO/IEC 27019 13.1.3 ISO/IEC 27001 A.12.2.1 ISO/IEC 27019 12.2.1	• Der Sicherheitsproxy sollte eine Schadsoftwareprüfung integrieren, sowie potenziell gefährliche Inhalte wie Active Content und bekannte Schadsoftware-URLs ausfiltern und regelmäßig aktualisiert werden.
A 3.2.3	Virtuelle Schleuse	Siehe A.3.2.1	ISO/IEC 27001 A.12.2.1 ISO/IEC 27019 12.2.1	• Für die Realisierung können auch sog. ReCoBs-Systeme (Remote Controlled Browser) verwendet werden.
A 3.2.4	Sichere Dokumentenerstellung	In Dokumenten, die aus dem Internet heruntergeladen oder per E-Mail eingehen, müssen unsichere Makro-Funktionen herausgefiltert bzw. deaktiviert werden. Ebenso müssen die Authentizität und Integrität von über das Internet ausgetauschten Dokumenten sichergestellt werden, z.B. durch Signierung.		
A 3.2.5	Detektionswerkzeuge für gezielte Angriffe auf Webseiten bzw. E-Mails	Eingehende E-Mail sowie der Internet-Verkehr müssen auf gezielte Angriffe hin überwacht werden.	ISO/IEC 27001 A.12.2.1 ISO/IEC 27019 12.2.1	
A 3.2.6	Security Information and Event Management (SIEM)	Der Internetzugriff aus Netzwerken zur Messung, Überwachung, Steuerung und Regelung des kDL-Teilpro-	ISO/IEC 27001 A.12.4.1 ISO/IEC 27019 12.4.1	• Siehe hierzu auch BDEW/OE Whitepaper, 4.5.6 Logging

		zesses SBeL und die zugehörige Infrastruktur muss mittels eines SIEM überwacht werden.		

Sichere Software (insbesondere Vermeidung von offenen Sicherheitslücken)				
Referenz	**Maßnahme**	**Anforderung**	**Norm-Kapitel**	**Beispiele und Hinweise**
A 3.3.1	Spam-Abwehr, Content Filtering	Unsichere Inhalte sowie Spam muss in eingehender E-Mail ausgefiltert werden. Siehe auch A 3.2.2.	ISO/IEC 27001 A.12.2.1 ISO/IEC 27019 12.2.1 ISO/IEC 27001 A.13.1.2	• Der Filter-Lösung sollte eine Schadsoftwareprüfung integrieren, sowie potenziell gefährliche Inhalte wie Active Content und bekannte Schadsoftware-URLs ausfiltern und regelmäßig aktualisiert werden.
A 3.3.2	Toolunterstützte Inventarisierung von Hardware und Software	Die eingesetzten Hard- und Softwareversionen müssen erfasst werden.	ISO/IEC 27001 A.8.1.1 ISO/IEC 27019 8.1.1 ISO/IEC 27019 12.6.1	• Siehe hierzu auch BDEW/OE Whitepaper, 4.4.3 Dokumentation der Netzwerkstruktur und -konfiguration • Umfang und Detaillierungsgrad der Inventarisierung sollten so gewählt werden, dass insbesondere ein zeitnahes Patchmanagement ermöglicht wird.
A 3.3.3	Zentrales Patch- und Änderungsmanagement, Konfigurationsmanagement	Es muss ein zentrales Patch- und Änderungsmanagement sowie ein Konfigurationsmanagement umgesetzt werden.	ISO/IEC 27001 A.12.1.2 ISO/IEC 27019 12.1.2 ISO/IEC 27001 A.12.5.1 ISO/IEC 27019 12.5.1 ISO/IEC 27019 12.6.1 ISO/IEC 27001 A.14.2.2	• Siehe hierzu auch BDEW/OE Whitepaper, 4.1.2 Patchfähigkeit und Patch-Management, 4.1.3 Bereitstellung von Sicherheits-Patches für alle Systemkomponenten und 4.7.3 Konfigurations- und Change-Management, Rollbackmöglichkeiten

A 3.3.4	Schutz vor Schadsoftware	Es muss ein Schadsoftwareschutz umgesetzt werden.	ISO/IEC 27001 A.12.2.1 ISO/IEC 27019 12.2.1	• Siehe hierzu auch BDEW/OE Whitepaper, 4.3.2 Schadsoftware-Schutz und 4.4.1 Grundsicherung und Systemhärtung
A 3.3.5	Softwaretest und Freigabe	Vor der Installation neuer Softwareversionen müssen diese auf Erfüllung der funktionalen und Security-Anforderungen geprüft und freigegeben werden.	ISO/IEC 27001 A.12.5.1 ISO/IEC 27019 12.5.1 ISO/IEC 27001 A.12.6.2 ISO/IEC 27001 A.14.2.2 ISO/IEC 27001 A.14.2.3 ISO/IEC 27001 A.14.2.4 ISO/IEC 27001 A.14.2.8 ISO/IEC 27001 A.14.2.9	• Siehe hierzu auch BDEW/OE Whitepaper, 4.2.2 Sicherheits- und Abnahmetests und 4.6.1 Sichere Entwicklungsstandards, Qualitätsmanagement und Freigabeprozesse
A 3.3.6	Software Development Security (sichere Software-Entwicklung)	Interne oder externe Software-Entwicklung muss unter Berücksichtigung definierter Security-Mindestvorgaben erfolgen.	ISO/IEC 27001 A.14.2.1 bis A.14.2.9	• Siehe hierzu auch BDEW/OE Whitepaper, 4.6 Entwicklung
A 3.3.7	Security Operation	Es müssen Prozesse zur Überwachung eines sicheren Betriebs mit einem regelmäßigen Reporting etabliert werden sein.	ISO/IEC 27001 A.12.1.1 bis A.12.7.1	
A 3.3.8	Sichere Beschaffung und Aussonderung (sicheres Löschen, Überwachung, Datensicherung und -wiederherstellung (Backup), Archivierung)	Beschaffung und Aussonderung muss unter Berücksichtigung definierter Security-Mindestvorgaben erfolgen.	ISO/IEC 27001 A.8.3.2 ISO/IEC 27001 A.14.1.1 ISO/IEC 27019 14.1.1	• Zur Definition von konkreten Sicherheitsvorgaben im Rahmen des Beschaffungsprozesses wird die Nutzung des BDEW/OE-Whitepapers empfohlen

Sichere Authentisierung				
Referenz	**Maßnahme**	**Anforderung**	**Norm-Kapitel**	**Beispiele und Hinweise**
A 3.4.1	Identitäts- und Rechtemanagement	Identitäten und Rechte müssen durch einen gesteuerten Prozess verwaltet werden.	ISO/IEC 27001 A.6.1.2 ISO/IEC 27001 A.9.1.1 ISO/IEC 27019 9.1.1 ISO/IEC 27001 A.9.2.1 bis A.9.2.6 ISO/IEC 27019 9.2.1	• Siehe hierzu auch BDEW/OE Whitepaper, 4.5.1 Rollenkonzepte
A 3.4.2	Multifaktor-Authentisierung (Zweifaktor-Authentisierung)	Zugriff auf Netzwerke, Systeme und Applikationen zur Messung, Überwachung, Steuerung und Regelung des kDL-Teilprozesses SBeL darf nur nach einer Multifaktor-Authentisierung oder einer anderen, äquivalenten Mehrfachsicherung möglich sein.	ISO/IEC 27001 A.9.4.2 ISO/IEC 27019 9.4.2	• Siehe hierzu auch BDEW/OE Whitepaper, 4.5.2 Benutzer-Authentifizierung und Anmeldung
A 3.4.3	Zugriffskontrolle (Sicheres Logon)	Siehe A 3.4.2		
A 3.4.4	Rollentrennung (Getrennte Admin-Konten)	Es muss ein Rollenkonzept umgesetzt sein, dass die Nutzung separater Konten für die Durchführung von privilegierten und nicht-privilegierten Tätigkeiten vorsieht.	ISO/IEC 27001 A.9.1.1 ISO/IEC 27019 9.1.1 ISO/IEC 27001 A.9.2.3 ISO/IEC 27001 A.9.4.4	• Siehe hierzu auch BDEW/OE Whitepaper, 4.5.1 Rollenkonzepte

Verschlüsselung				
Referenz	**Maßnahme**	**Anforderung**	**Norm-Kapitel**	**Beispiele und Hinweise**
A 3.5.1	Kryptografische Absicherung (data in rest, data in motion)	Vertrauliche Daten, deren Offenlegung den kDL-Teilprozess SBeL gefährden kann, müssen verschlüsselt übertragen und gespeichert werden.	ISO/IEC 27001 A.8.3.1 ISO/IEC 27001 A.10.1.1 ISO/IEC 27019 13.1.4 ENR	• Siehe hierzu auch BDEW/OE Whitepaper, 4.1.5 Verschlüsselung vertraulicher Daten, 4.1.6 Kryptographische Verfahren und 4.2.3 Sichere Datenspeicherung und Übertragung
A 3.5.2	Cloud-Daten-Verschlüsselung (Cloud-Encryption)	Vertrauliche Daten, deren Offenlegung den kDL-Teilprozess SBeL gefährden kann, dürfen bei der Nutzung von Cloud-Diensten nur verschlüsselt übertragen und gespeichert werden.	ISO/IEC 27001 A.10.1.1 ISO/IEC 27001 A.10.1.2 ISO/IEC 27019 10.1.2 ISO/IEC 27001 A.15.1.2 ISO/IEC 27019 15.1.2 ISO/IEC 27001 A.15.1.3	• Siehe hierzu auch BDEW/OE Whitepaper, 4.1.5 Verschlüsselung vertraulicher Daten, 4.1.6 Kryptographische Verfahren und 4.2.3 Sichere Datenspeicherung und Übertragung • Siehe hierzu auch UP KRITIS „Best-Practice-Empfehlungen für Anforderungen an Lieferanten zur Gewährleistung der Informationssicherheit in kritischen Infrastrukturen“
A 3.5.3	Verschlüsselung der Kommunikationsverbindungen (z.B. Voice Encryption)	Vertrauliche Daten, deren Offenlegung den kDL-Teilprozess SBeL gefährden kann, dürfen über öffentliche Kommunikationsverbindungen nur verschlüsselt übertragen werden.	ISO/IEC 27001 A.10.1.1 ISO/IEC 27019 13.1.4 ENR	• Siehe hierzu auch BDEW/OE Whitepaper, 4.1.5 Verschlüsselung vertraulicher Daten, 4.1.6 Kryptographische Verfahren, 4.2.3 Sichere Datenspeicherung und Übertragung und 4.4.1 Eingesetzte Protokolle und Technologien
A 3.5.4	E-Mail-Verschlüsselung	Vertrauliche Daten, deren Offenlegung den kDL-Teilprozess SBeL gefährden	ISO/IEC 27001 A.10.1.1	• Siehe hierzu auch BDEW/OE Whitepaper, 4.1.5 Verschlüsselung vertraulicher Daten, 4.1.6 Kryptographische

		kann, dürfen nur verschlüsselt per E-Mail übertragen werden.		Verfahren, 4.2.3 Sichere Datenspeicherung und Übertragung
A 3.5.5	Verschlüsselung der Datenträger z. B. Festplattenverschlüsselung	Vertrauliche Daten, deren Offenlegung den kDL-Teilprozess SBeL gefährden kann, dürfen nur verschlüsselt gespeichert werden.	ISO/IEC 27001 A.8.3.1 ISO/IEC 27001 A.10.1.1	• Siehe hierzu auch BDEW/OE Whitepaper, 4.1.5 Verschlüsselung vertraulicher Daten, 4.1.6 Kryptographische Verfahren, 4.2.3 Sichere Datenspeicherung und Übertragung

Physische Sicherheit				
Referenz	**Maßnahme**	**Anforderung**	**Norm-Kapitel**	**Beispiele und Hinweise**
A 3.6.1	Zugangskontrolle	Der Zugang und Zutritt zu Netzwerk- und Systemkomponenten, die der Messung, Überwachung, Steuerung und Regelung des kDL-Teilprozesses SBeL dienen, muss durch eine Zutrittskontrolle geschützt sein.	ISO/IEC 27001 A.11.1.1 bis A.11.1.6 ISO/IEC 27019 11.1.1 ISO/IEC 27019 11.1.7 ENR ISO/IEC 27019 11.1.8 ENR	
A 3.6.2	Notstromversorgung (USV)	Netzwerk- und Systemkomponenten, die der Messung, Überwachung, Steuerung und Regelung des kDL-Teilprozesses SBeL dienen, müssen durch eine USV und Netzersatzanlage abgesichert sein.	ISO/IEC 27001 A.11.2.2 ISO/IEC 27019 11.2.2	
A 3.6.3	Netzersatzanlagen	Siehe A 3.6.2	-	

Weitere Maßnahmen				
Referenz	**Maßnahme**	**Anforderung**	**Norm-Kapitel**	**Beispiele und Hinweise**
A 3.7.1	Sensibilisierung und Schulungen	Es muss ein Schulungskonzept realisiert sein, das regelmäßige Informationssicherheitsschulungen und Sensibilisierungsmaßnahmen für alle relevanten internen und externen Mitarbeiter vorsieht.	ISO/IEC 27001 A.7.2.2 ISO/IEC 27019 7.2.2	
A 3.7.2	Übungen	Notfallkonzepte und Datenwiederherstellungsverfahren müssen durch Übungen in regelmäßigen Abständen getestet werden. Ferner kann das erfolgreiche Durchlaufen des Aufbaus einer Kommunikationsverbindung zur Übung einer Meldung eines meldepflichtigen IT-Sicherheitsvorfalls (Testvorfall), angelehnt an § 8b Absatz 4 BSIG, regelmäßig durchgeführt werden.	ISO/IEC 27001 A.12.3.1 ISO/IEC 27001 A.17.1.3	• Siehe hierzu auch Abschnitt 5.4
A 3.7.3	Aufrechterhaltung des aktuellen Informationsstands durch Bezug von Warnungen, CERT-Meldungen, Lagebild	Der Betreiber muss sicherstellen, dass er jederzeit über einen aktuellen Informationsstand bezüglich der für den Aggregatorbetrieb relevanten Informationssicherheitslage verfügt.	ISO/IEC 27001 A.6.1.3 ISO/IEC 27019 6.1.3 ISO/IEC 27001 A.6.1.4 ISO/IEC 27019 6.1.4 ISO/IEC 27001 A.16.1.6	• Es sollte eine Mitgliedschaft in Sicherheitsarbeitskreisen von BDEW und UP KRITIS geprüft werden • Zur Information über aktuelle Softwareschwachstellen sollte ein Benachrichtigungsdienst des Herstellers oder eines externen Dienstleisters genutzt werden

				• Warn- und Informationsdienst (WID) des CERT-Bunds
A 3.7.4	Verfügbarkeit notwendiger Ressourcen	Der Betreiber muss sicherstellen, dass jederzeit die notwendigen Ressourcen für einen den Anforderungen dieses B3S entsprechenden Aggregator-Betriebs zur Verfügung stehen.	ISO/IEC 27001 7.1	
A 3.7.5	Interne Audits und Penetrationstests	Durch regelmäßige interne Audits und technische Sicherheitstests muss überprüft werden, dass die Anforderungen dieses B3S eingehalten werden.	ISO/IEC 27001 A.18.2.1 ISO/IEC 27001 A.18.2.2 ISO/IEC 27001 A.18.2.3 ISO/IEC 27019 18.2.3	• Siehe hierzu auch BDEW/OE Whitepaper, 4.2.2 Sicherheits- und Abnahmetests und 4.3.1 Grundsicherung und Systemhärtung
A 3.7.6	Sicherheitsstrategie und Sicherheitsleitlinie	Die Umsetzung der wesentlichen Anforderungen dieses B3S muss in einer Sicherheitsstrategie bzw. Sicherheitsleitlinie dokumentiert werden.	ISO/IEC 27001 5.2 ISO/IEC 27001 A.5.1.1	