AGFW | Der Energieeffizienzverband für Wärme, Kälte und KWK e.V.
Stresemannallee 30
60596 Frankfurt am Main

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

Branchenspezifischer Sicherheitsstandard für die Verteilung von Fernwärme (B3S VvFw)

Nach § 8a Abs. 2 BSI-Gesetz

Stand: 15. Februar 2021

Version 1.1

Inhaltsverzeichnis

Abkürzungsverzeichnis

AGFW	AGFW I Der Energieeffizienzverband für Wärme, Kälte und KWK e.V.
AGFW-TSM	Zertifizierungsverfahren zum Technischen Sicherheits-management des AGFW
ASCII	American Standard Code for Information Interchange (Amerikanischer Standard-Code für den Informationsaustausch
APT	Advanced Persistent Threat (fortgeschrittene, andauernde Bedrohung), eine Form von Angriff, bei der der Angreifer möglichst lange unentdeckt bleiben will, um in den Besitz möglichst vieler Informationen zu gelangen, um seinen Angriff vorzubereiten.
AVBFernwärmeV	AVB Fernwärme Verordnung
B3S	Branchenspezifische Sicherheitsstandards
BCM	Business Continuity Management
BDEW	Bundesverband der Energie- und Wasserwirtschaft e.V.
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSI KritisV	Verordnung zur Bestimmung Kritischer Infrastrukturen
DDoS	Distributed-Denial-of-Service (spezielle Art von Cyber-Kriminalität)
DIN	Deutsches Institut für Normung
Fernwirktechnik	kommunikationstechnisches Verfahren, gleich Übertragungstechnik
GmbH	Gesellschaft mit beschränkter Haftung
IDS	Intrusion Detection System
IEC	Internationale Elektrotechnische Kommission
IPS	Intrusion Prevention System
ISMS	Informationssicherheitsmanagementsystem
ISO	International Organization for Standardization
ISO/IEC 27001	International führende Norm für Informationssicherheits-Managementsysteme

IT	Beinhaltet nach § 8a Abs. 1 Satz 1 BSIG: „informationstechnische Systeme, Komponenten oder Prozesse“
ITK	Informations- und Telekommunikationstechnik
kDL	Kritische Dienstleistung
KRITIS	Kritische Infrastrukturen
MODBUS	Modbus ist ein Anwendungsprotokoll für den Austausch von Nachrichten zwischen intelligenten Modbus-Controllern
PDCA	Plan/Planen, Do/Durchführen, Check/Überprüfen, Act/Handeln
RL	Rücklauf
RTU	Remote Terminal Unit (Fernbedienungsterminal)
SCADA	Supervisory Control and Data Acquisition (Überwachen und Steuern technischer Prozesse mittels eines Computer-Systems)
SPS	Speicherprogrammierbare Steuerung
TCP/IP	Transmission Control Protocol/Internet Protocol (ist eine Familie von Netzwerkprotokollen und wird wegen ihrer großen Bedeutung für das Internet auch als Internetprotokollfamilie bezeichnet)
Übertragungstechnik	kommunikationstechnischen Verfahren, gleich Fernwirktechnik
VGB PowerTech	Verband der Großkraftwerksbetreiber e.V.
VL	Vorlauf
VPN	Virtuelles privates Netzwerk
VvFw	Verteilung von Fernwärme

1 Allgemeines

1.1 Anwendungsbereich

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

Der B3S Verteilung von Fernwärme (B3S VvFw) legt fest, dass die nachhaltige und angemessene Behandlung aller relevanten Themenfelder zur Umsetzung der gesetzlichen Anforderungen nach § 8a Abs. 1 BSIG, z.B. durch den Betrieb eines Informationssicherheitsmanagementsystems (ISMS) in Anlehnung an ISO/IEC 27001 sichergestellt wird. Der B3S VvFw findet Anwendung auf informationstechnische Systeme, Komponenten oder Prozesse der Kritischen Infrastruktur Fernwärmenetz, d.h. auf IT-Systeme der Prozessdatenverarbeitung zur Messung, Steuerung und Regelung, die für die Funktionsfähigkeit der kritischen Dienstleistung (kDL) Verteilung von Fernwärme (VvFw) maßgeblich sind.

Der B3S VvFw gilt für Fernwärmenetze, die den Schwellenwert nach Anhang 1 Teil 3 Tabelle 4.2.1 BSI-KritisV erreichen oder überschreiten und damit als KRITIS eingestuft worden sind. Die kritische Dienstleistung (kDL) in diesem Sinne ist die Verteilung von Fernwärme (VvFw).

Die leitungsgebundene Verteilung von Fernwärme steht im direkten Wettbewerb zu anderen Formen der Wärmeversorgung, z.B. Öl- oder Gaszentralheizungen, Blockheizkraftwerken, Wärmepumpen, Holzheizungen, Solarthermieanlagen usw. In einer Kommune, Stadt bzw. Gemeinde können mehrere voneinander unabhängige Fernwärmenetze bestehen, deren Betreiber in der Regel im Wettbewerb stehen. Bei der Fernwärmeversorgung gibt es im Gegensatz zur Strom- und Gasversorgung keine Grundversorgungspflichten.

Als Fernwärmeverteilung bezeichnet man die Versorgung von baulichen Anlagen mit Wärme über Liegenschaftsgrenzen hinweg. Fernwärme wird in Form von heißem Wasser oder in Einzelfällen auf Basis von Dampf verteilt. Das Fernheizwasser fließt in einem Kreislaufsystem von den Wärmeerzeugungsanlagen (Heizkraftwerke und Heizwerke) zum Kunden und zurück. Die meisten Heizkraftwerke und Heizwerke geben ihre Wärme an gemeinsame Fernwärmenetze ab (vermaschte Verbundnetze). Im vermaschten Verbundnetz kann durch Schaltmaßnahmen der Ausfall einer Versorgungsleitung (z. B. durch Rohrbruch) kompensiert werden, indem die Versorgung der Kunden mit Wärme - bis auf die unmittelbare Schadensumgebung - über andere Rohleitungsstränge bzw. durch das Auftrennen des Verbundnetzes in Inselnetze aufrechterhalten bleibt.

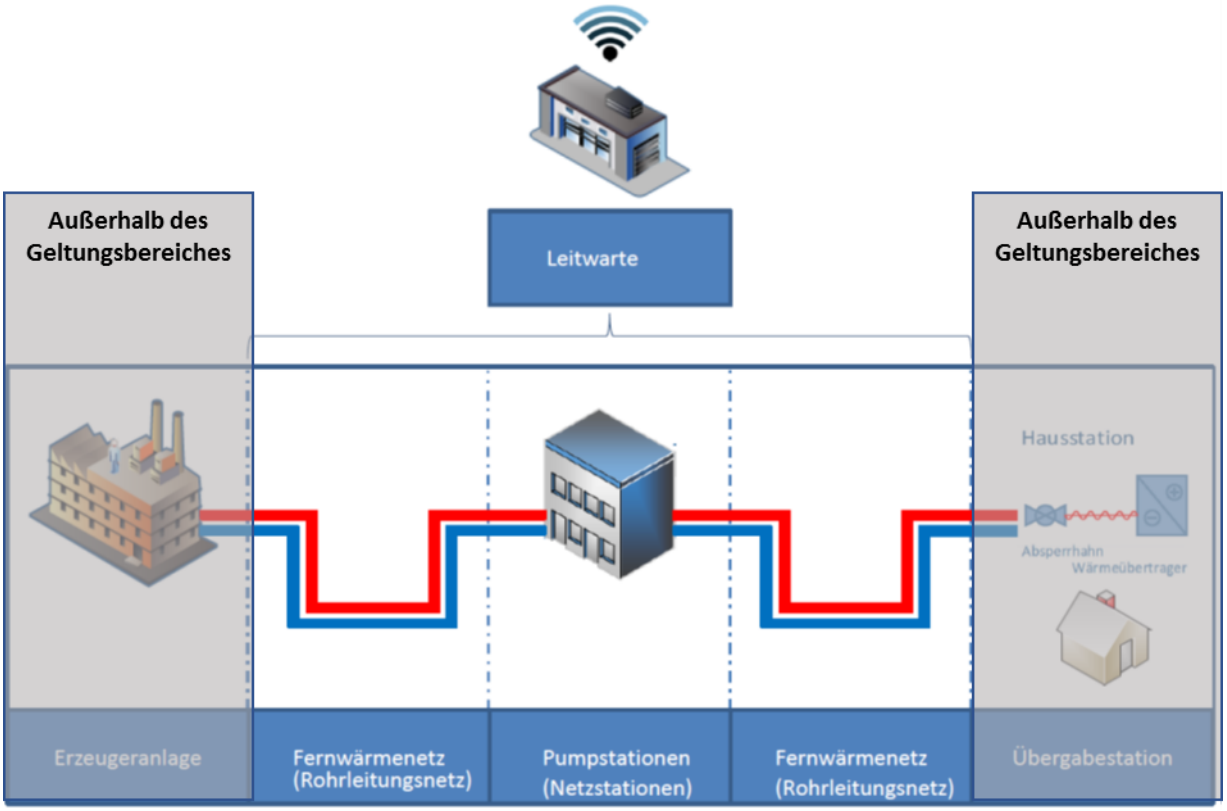

Abbildung 1: Darstellung Fernwärmenetz

Fernwärmenetze bestehen aus den folgenden fünf wesentlichen Baugruppen (siehe Abbildung 1:

1. Dem eigentlichen Rohrleitungsnetz, bestehend aus einem Vorlauf zur Verteilung des heißen Fernheizwassers und einem Rücklauf zur Rückführung des abgekühlten Fernheizwassers. (Zweileiternetz: einzelner Vorlauf speist parallel die Raumheizung und die Warm- bzw. Brauchwasserbereitung sowie einzelner Rücklauf. In Einzelfällen existieren auch Dreileiternetze, die über zwei Vorlaufleitungen verfügen, einen für die Raumheizung und einen als Konstantwärmeleiter für die hausinterne Warmwasserbereitung)
2. Den Pumpstationen mit Pumpen zur Druckerhöhung im Fernwärmenetz. Die Druckerhöhung dient zur Überwindung von Druckverlusten im Fernwärmenetz und damit zum Transport der Fernheizwassermengen. Pumpen können entweder analog oder digital gesteuert werden. Bei einer digitalen Steuerung sorgen IT-Systeme (z.B. SPS) für die Funktionsfähigkeit, bei analoger Steuerung können die Pumpen komplett manuell vor Ort bedient werden. Zur Umsetzung einer betriebswirtschaftlich optimierten Steuerung kann die digitale Steuerung der Pumpen über Fernwirktechnik mit einer zentralen Leitwarte verbunden und von dort fernbedient werden. Die Übertragung kann

über das Internet oder über von der Öffentlichkeit vollkommen getrennte Übertagungstechnik erfolgen.

3. Der Leitwarte zur Netzsteuerung, zuständig für die Überwachung und ggf. die Steuerung der Fernwärmeversorgung. Ihr obliegt die optimierte Fahrweise, auch unter dem Gesichtspunkt der Wirtschaftlichkeit. Die Steuerung reagiert in der Regel auf Signale einer Druckmessung bzw. Druckdifferenzmessung. Bei Laständerung in der Fernwärme kann u.a. durch manuellen Eingriff die Fördermenge der Pumpstationen über die Fernwirktechnik angepasst werden. Die Fördermenge wird durch Ändern der Pumpendrehzahl und/oder die An-/Abfahrt von Pumpen geregelt. Der Signalaustausch erfolgt über die Fernwirktechnik. Eine zentrale Aufgabe ist die Gewährleistung einer wirtschaftlich optimierten Fahrweise des Fernwärmenetzes.
4. Der zentralen Leittechnik (Netzleitsystem), die das Leitwarten-Personal bei der Überwachung und Steuerung des Fernwärmenetzes unterstützt. Über die zentrale Leittechnik werden Komponenten im Fernwärmesystem gesteuert. Zudem werden Störmeldungen aus dem Fernwärmenetz dargestellt und können so effizient abgearbeitet werden.
5. Der Übergabestation (technische Einrichtung) als Bindeglied zwischen Rohrleitungsnetz und Hauszentrale des Kunden. Sie befindet sich in der Regel im Verantwortungsbereich und Gebäude des Kunden und dient dazu, die Wärme bestimmungsgemäß, z. B. hinsichtlich Druck, Temperatur und Volumenstrom, an die Hauszentrale zu übergeben.

1.2 Geltungsbereich

Bei der kDL VvFw handelt es sich um die direkte Einflussnahme auf die Einspeisung, Durchleitung und Entnahme von Fernheizwasser oder Dampf in das bzw. aus dem Fernwärmenetz.

Maßgebliche Infrastrukturen und Ressourcen im Geltungsbereich

Der Geltungsbereich des B3S VvFw beinhaltet alle informationstechnischen Systeme, Komponenten und Prozesse des Fernwärmenetzes, die für den Betrieb der kDL maßgeblich sind. Hierzu zählen unter anderem:

- die zur Messung, Überwachung, Steuerung und Regelung maßgeblichen zentralen und dezentralen IT-Infrastrukturen und Prozesse (z.B. SCADA-Applikationen, Regelungs- / Steuerungskomponenten, Energiedatenmanagementsysteme zur Steuerung und Überwachung, Schnittstellen zum Steuer- / Leitsystem).
- die zum Betrieb der oben genannten IT-Infrastrukturen maßgeblichen Netzwerkkomponenten.
- die maßgeblichen Betriebsstandorte des Fernwärmenetzes wie z. B. Pumpstationen, Leitwarten, Rechenzentren, Technikräume, etc. die für den Betrieb der vorstehenden Systeme durchführungsverantwortlichen Personen bzw. Organisationseinheiten.

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

Der Geltungsbereich („Scope“) des ISMS muss die hier aufgeführten Kategorien von Anwendungen, Systemen, Komponenten, Betriebsstandorten und Personen bzw. Organisationseinheiten umfassen.

Außerhalb des Geltungsbereiches des B3S VvFw

Nicht zum Geltungsbereich des vorliegenden B3S VvFw gehören:

- der kDL VvFw vorgelagerte dezentrale Systeme und Abläufe zur Bereitstellung der Wärme in den Erzeugungs- / Einspeiseanlagen (z.B. Heizkraftwerke, Heizwerke und Dritteinspeiser).
- der kDL VvFw nachgelagerte Systeme und Abläufe des Fernwärmevertriebs und Kundenservices (z.B. Datenauskoppelung zur Bereitstellung an Dritte).
- Übergabestationen und Hausanlagen, d.h. die Anlagen auf Seiten des Kunden
- das Rohrleitungsnetz, wenn dort keine IT-Einrichtungen zum Einsatz kommen.

1.3 Geltungsbereich für extern erbrachte Leistungen

Werden Anwendungen, Systeme und Komponenten, die der Anwendung dieses B3S VvFw unterliegen, nicht vom Fernwärmenetzbetreiber selbst betrieben, sondern von Dritten, beispielsweise im Rahmen von Outsourcing, so ist die Anwendung und Umsetzung dieses B3S VvFw durch entsprechende Vereinbarungen sicherzustellen. Die Verantwortung in Bezug auf die Einhaltung des B3S VvFw bleibt dabei beim Betreiber des Fernwärmenetzes (z.B. durch Abschluss einer Dienstleistervereinbarung, deren Inhalt und Umsetzung geprüft wird).

1.4 Gesetzlicher Rahmen

Die AVBFernwärmeV ist die Vertragsgrundlage für die Fernwärmelieferung an Endkunden.

2 Schutz der kritischen Dienstleistung (KRITIS-Schutzziel)

Das Schutzziel der kDL Fernwärmeversorgung gemäß der BSI-KritisV ist die Versorgung der Allgemeinheit mit Fernwärme, insbesondere im Winter während der Heizperiode. Die Fernwärmeversorgung wird durch die Erzeugung und die Verteilung von Fernwärme (VvFw) erbracht. Dieser B3S besteht für den Teilbereich der Verteilung von Fernwärme (VvFw).

Zur Erfüllung der kritischen Dienstleistung „Verteilung von Fernwärme“ muss die Verfügbarkeit und Funktionsfähigkeit der maßgeblichen Infrastrukturen zum Transport des Wassers oder des Dampfes zur Fernwärmeversorgung gewährleistet werden.

Maßnahmen zur Erfüllung des KRITIS-Schutzziels gemäß dieses B3S VvFw beziehen sich ausschließlich auf informationstechnische Systeme, Komponenten oder die Prozesse, die für die Funktionsfähigkeit der kDL maßgeblich sind. Diese müssen die Anforderungen der nachfolgend definierten IT-Schutzziele in angemessener Form erfüllen.

2.1 IT-Schutzziele

IT-Schutzziele sind die Gewährleistung und Aufrechterhaltung der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der informationstechnischen Systeme, Komponenten oder Prozesse, die für die Funktionsfähigkeit der betriebenen kritischen Infrastrukturen maßgeblich sind. Entsprechend sind angemessene organisatorische und technischer Vorkehrungen zu deren Sicherstellung zu treffen.

2.2 Branchenspezifischer IT-Schutzbedarf

Der Schutzbedarf für informationstechnische Systeme, Komponenten oder Prozesse, sofern diese für die Funktionsfähigkeit der betriebenen kritischen Infrastrukturen maßgeblich sind, leitet sich aus den IT-Schutzzielen unter Berücksichtigung des KRITIS-Schutzziels ab und ist somit erschöpfend.

Für die IT-Systeme, und bei Vorhandensein für die Fernwirktechnik, sind folgende anlagenspezifische Schutzziele zu berücksichtigen:

1) Verfügbarkeit: Bedeutet, dass bei einer digitalen Steuerung der Komponenten des Fernwärmenetzes die hierfür verwendeten IT-Systeme und Fernwirktechniken verfügbar, d.h. funktionsfähig, sind.
2) Integrität: Bedeutet, dass digitale Messwerte, die vom IT-System ausgehen, im Rahmen des Übertragungsprotokolls fehlerkorrigiert, d.h. unverfälscht, in der Leitwarte ankommen und umgesetzt werden, sowie digitale Steuerwerte der Leitwarte wiederum entsprechend beim IT-System ankommen und umgesetzt werden.
3) Authentizität: Bezeichnet die Eigenschaften der Echtheit, Überprüfbarkeit und damit Vertrauenswürdigkeit des Senders von übermittelten Daten. Diese Überprüfung wird als Authentifikation bezeichnet und weist nach, dass Daten tatsächlich von dem angegebenen Sender (z.B. der SPS oder der Leitwarte) übermittelt wurden.

4) Vertraulichkeit: Beinhaltet den Schutz vor unbefugter Freigabe von Informationen und Daten der IT-Systeme an Dritte. Dies ist für die Erbringung der kDL VvFw jedoch nur in Ausnahmefällen von Relevanz.

Bei der Bewertung der KRITIS-Schutzziele ist zu berücksichtigen, dass die Speicherwirkung der mit Fernwärme versorgten Gebäude bzw. die Trägheit des gesamten Fernwärme-Systems in der Regel eine Total-Ausfallzeit der Fernwärmeversorgung zwischen 3-5 Stunden ohne Komfortverlust in den Wohnungen erlaubt. Erst nach 24 Stunden stellt sich eine spürbare Raumtemperaturabsenkung ein.

2.3 Maßgeblichkeit der IT

Die IT des Betreibers ist für die Funktionsfähigkeit der Fernwärme-Verteilung maßgeblich, wenn

- diese für den Regelbetrieb (bestimmungsgemäßer Betrieb) zur Verteilung der Fernwärme an Haushalte unabdingbar ist und
- diese angeschlossenen Haushalte im Falle einer Störung oder eines Ausfalls der eingesetzten IT über einen Zeitraum von 24 Stunden keine Wärmelieferung an der Übergabestation erhalten.

Sollten die o.g. Voraussetzungen zutreffen, kann davon ausgegangen werden, dass ohne die maßgebliche IT die kritische Dienstleistung nicht mehr erbracht werden kann. Die etwaige Maßgeblichkeit der IT muss durch den Betreiber der Kritischen Infrastruktur festgestellt werden.

Wenn für die Funktionsfähigkeit der kDL VvFw informationstechnische Systeme, Komponenten oder Prozesse nicht maßgeblich sind, z.B. sie nur der wirtschaftlichen Fahrweise dienen, weil die relevanten Steuerungsmechanismen manuell (d.h. ohne digitale Informations- und Steuerungstechnik) jederzeit vor Ort in den Pumpstationen bedient werden können, entfällt die Betrachtung und Behandlung der Risiken in Bezug auf die IT-Schutzziele.

In diesem Fall muss die Nicht-Maßgeblichkeit der IT durch den Betreiber der kritischen Infrastruktur im Rahmen der Risikobetrachtung nachgewiesen werden. Der Nachweis umfasst insbesondere die Beschreibung der organisatorischen und technischen Maßnahmen, welche ermöglichen, dass die VvFw auch ohne IT manuell aufrechterhalten werden kann.

Der Nachweis umfasst ferner die Bestätigung der Wirksamkeit dieser Maßnahmen, z.B. über eine AGFW-TSM-Zertifizierung gemäß Arbeitsblatt AGFW FW 1000.

3 Risikomanagement

Das Risikomanagement umfasst für diesen B3S VvFw in Anlehnung an die ISO 31000 zumindest die Risikoidentifikation, die Risikoanalyse, die Risikobewertung und die Risikobehandlung. Weitere anwendbare Standards sind beispielsweise ISO/IEC 27005 und BSI-Standard 200-3.

3.1 Dokumentation des Anwendungsbereiches

Vor Beginn der Risikoanalyse müssen alle informationstechnischen Systeme, Komponenten oder Prozesse, die maßgeblich für die Funktionsfähigkeit der kDL VvFw sind, identifiziert, beschrieben und dokumentiert werden. Zudem sind Schnittstellen zu oder Abhängigkeiten von anderen Systemen kenntlich zu machen, da deren mögliche Veränderung ggf. Auswirkungen auf die IT im Anwendungsbereich haben könnte.

3.2 Business Impact Analyse

Die Business Impact Analyse (BIA) bildet die Grundlage für die spätere Risikoanalyse und -behandlung. Sie ermittelt die Auswirkungen, die eine Verletzung der Schutzziele auf die Erbringung der kritischen Dienstleistung haben könnte.

Die BIA beginnt mit der Ermittlung der Informationswerte, die zur Erbringung der kritischen Dienstleistung erforderlich sind (z.B. Steuerungsvorgaben, Messwerte, Meldungen o.Ä.). Danach erfolgt eine Zuordnung der Informationswerte zu der informationstechnischen Infrastruktur (Systeme, Komponenten oder Prozesse), mit der Informationen übertragen und verarbeitet werden.

Im folgenden Schritt werden für alle Informationswerte die möglichen Schadensauswirkungen auf die kDL VvFw bei Verletzung der relevanten Schutzziele (Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit) bewertet. Die entsprechend zugehörige Infrastruktur erhält zumindest die Bewertung der Informationen, die darauf verarbeitet werden. Für die Einordnung der Auswirkungen sind geeignete Schadensabstufungen zu verwenden z.B. „gering“, „mäßig“, „hoch“ und „kritisch“. Die genaue Festlegung der Schadenskategorien und deren Bedeutung für die VvFw ist vom Anwender dieses B3S VvFw im Vorfeld der Business Impact Analyse zu definieren.

3.3 Branchenspezifische Gefährdungslage

Eine Gefährdung im Sinne des B3S VvFw beschreibt eine Situation oder einen Sachverhalt, der durch Einwirkung auf informationstechnische Systeme, Komponenten oder Prozesse zu einer Verletzung der Schutzziele der Informationssicherheit mit Auswirkung auf die kDL VvFw führen kann (Schadensauswirkung gem. BIA siehe oben). Eine Gefährdung realisiert sich, indem eine Bedrohung eine Schwachstelle ausnutzt.

3.3.1 Allgefahrenansatz

Im Rahmen eines Allgefahrenansatzes sollen alle relevanten Bedrohungen und Gefährdungen identifiziert werden, die auf die maßgeblichen IT-Informationswerte im Geltungsbereich des B3S VvFw wirken. Aus den Gefährdungen werden Risiken für die kDL bestimmt, die im Rahmen der Risikoanalyse bewertet und behandelt werden müssen.

3.3.2 Branchenspezifische IT-relevante Gefährdungen

Die nachfolgende Tabelle führt mögliche Gefährdungen für informationstechnische Systeme, Komponenten oder Prozesse an, die maßgeblich für die Erbringung der kDL VvFw sind. Sie berücksichtigt u.a. im Rahmen der Umsetzung der Anforderungen aus der [ISO/IEC 27001] erkannte Gefährdungen und die des IT-Sicherheitskatalogs gem. §11 Absatz 1a EnWG:

Nr.	Branchenspezifische IT-relevante Gefährdungen	Relevanz für die kDL VvFw
1	**Elementare Gefährdungen (Naturgefahren)** *Beispiele für elementare Gefährdungen sind:* - Blitzeinschläge in oberirdischen Gebäuden - Hochwasser insb. in unterirdischen Pumpstationen (z.B. durch Starkregen oder sonstiger Wasseranstieg) - Wärme und/oder hohe Luftfeuchtigkeit - Gefährdung durch Feuer	*Elementare Gefährdungen können zu:* - Schädigung, Zerstörung oder Ausfall der ITK-Systeme zur Steuerung und/oder Überwachung der Pumpen und Leitsysteme führen
2	**Höhere Gewalt** *Beispiele für höhere Gewalt sind:* - Ausfall von Dienstleistern - Pandemie - Demonstrationen - Ausfall von öffentlichen Infrastrukturen/ Einrichtungen	*Höhere Gewalt kann zu:* - Zutrittsbeeinträchtigungen zu Betriebsstätten (z.B. Leitwarte, Pumpstation) führen - Nicht-Verfügbarkeit von Personal führen - Hinderung des ordnungsgemäßen Betriebes sowie Reaktion auf Probleme /

		Störungen (in kritischen Betriebszuständen) führen - Einschränkung in der Wartung des Leitsystems führen
3	**<u>Organisatorische Mängel</u>** *Beispiele für organisatorische Mängel sind:* - keine (IT-)Prozess-/ Richtlinienvorgaben - mangelnde Qualifikation/Schulungen - Fehlende Dienstleistersteuerung - Nichtverfügbarkeit von Personal	*Organisatorische Mängel können zu:* - Nicht-Beseitigung von Schwachstellen und dadurch potenzielle Schädigung, Zerstörung oder Ausfall der ITK-Systeme zur Steuerung und/oder Überwachung der Pumpen und Leitsysteme führen - menschlichen Fehlhandlungen (Falsch- und Nichthandlungen) führen - Verwendung von Daten oder Software aus nicht vertrauenswürdigen Quellen
4	**<u>Menschliche Fehlhandlungen</u>** *Beispiele für menschliche Fehlhandlungen sind:* - Fehlerhafte Steuerung, Administration und Bedienung von ITK-Systemen (fahrlässig / vorsätzlich/ erzwungen) - Nichteinhaltung von Vorgaben	*Menschliche Fehlhandlungen können zu:* - Schädigung, Zerstörung oder Ausfall der ITK-Systeme zur Steuerung und/oder Überwachung der Pumpen und Leitsysteme führen - fehlerhaften Steuerung des Fernwärmenetzes führen (Unterversorgung)
5	**<u>Versagen oder Beeinträchtigung anderer für die Anlagensteuerung relevanter Infrastrukturen (z.B. Fernwirktechnik) und externer Dienstleistungen</u>** *Beispiele für Versagen oder Beeinträchtigung anderer für die Anlagensteuerung relevanter*	*Versagen oder Beeinträchtigung anderer für die Anlagensteuerung relevanter Infrastrukturen und externer Dienstleistungen kann zu:* - Ausfall der Technik auf der Leitwarte oder der Fernwirktechnik führen, somit

	Infrastrukturen und externer Dienstleistungen sind: - Infrastrukturelle Mängel (z.B. Stromversorgung etc.) - Ausfall / Beeinträchtigung von passiven Übertragungsstrecken (z.B. Internetleitungen, Schächte etc.)	wäre keine Bedienung und Steuerung der Pumpen und Anlagen im Netz von der Leitwarte mehr möglich (Betriebsstörung) - Hinderung des ordnungsgemäßen Betriebes sowie Reaktion auf Probleme / Störungen (in kritischen Betriebszuständen) führen
6	**<u>Technisches Versagen von IT-Systemen</u>** *Beispiele für technisches Versagen von IT-Systemen sind:* - Dysfunktion (z.B. Fehlkonfiguration, Bugs etc.) in Software, oder Hardware - Verwendung ungeeigneter IT-Systeme und Komponenten	*Technisches Versagen von IT-Systemen kann zu:* - Ausfall der Technik auf der Leitwarte oder der Fernwirktechnik führen, somit wäre keine Bedienung und Steuerung der Pumpen und Anlagen im Netz von der Leitwarte mehr möglich (Betriebsstörung) - Hinderung des ordnungsgemäßen Betriebes sowie Reaktion auf Probleme / Störungen (in kritischen Betriebszuständen) führen
7	**<u>Gezielte IT-Angriffe</u>** *Beispiele für gezielte IT-Angriffe sind:* - Hacking und Manipulation - Social Engineering - gezielte Störung/ Verhinderung von Diensten - APT - Computer-Viren, Schadsoftware - Unbefugter Zugriff auf IT-Systeme und Daten	*Gezielte IT-Angriffe können zu:* - Manipulation von Daten und somit fehlerhafte oder beeinträchtigte Steuerung des Fernwärmenetzes führen (Unterversorgung) - unbefugtem Zugriff auf Nutzerzugänge zum Zweck der Manipulation oder Sperrung berechtigter Nutzer führen - Verfügbarkeitsausfällen der betroffenen Systeme (z.B. durch

	- Missbrauch von Fernzugangstechnik (remote access)	gezieltes Abschalten oder Systemüberlastung) führen
8	**<u>Gezielte Angriffe, Diebstahl oder Beschädigungen von Komponenten, Infrastruktur oder Ausrüstung mit Auswirkung auf die IT</u>** *Beispiele für gezielte Angriffe, Diebstahl oder Beschädigungen von Komponenten, Infrastruktur oder Ausrüstungen mit Auswirkung auf die IT sind:* - Extremistische und terroristische Akte, die zu Beschädigungen/Zerstörungen führen - Beschädigung und Zerstörung (physisch mit Wirkung auf die IT) - Diebstahl von IT-Equipment (PCs, mobile Endgeräte …) oder Infrastruktur die für den IT-Betrieb notwendig sind (Kabel, etc.) - Diebstahl von Ausrüstung	*Gezielte Angriffe, Diebstahl oder Beschädigungen von Komponenten, Infrastruktur oder Ausrüstung mit Auswirkung auf die IT können zu:* - Zutrittsbeeinträchtigungen zu Betriebsstätten (z.B. Leitwarte, Pumpstation) führen - Schädigung, Zerstörung oder Ausfall der ITK-Systeme zur Steuerung und/oder Überwachung der Pumpen und Leitsysteme führen - Hinderung des ordnungsgemäßen Betriebes sowie Reaktion auf Probleme / Störungen (in kritischen Betriebszuständen) führen - Verlust von Daten (z.B. aktuelle technische Daten, historische Werte des Leitsystems) führen
9	**<u>Datendiebstahl</u>** *Beispiele für Datendiebstahl sind:* - Abhören von Kommunikation - Ausspähen/ Aufzeichnen von Daten (inkl. dem nicht autorisierten Zugriff auf Nutzerkonten) - Umleiten von Datenströmen	*Datendiebstahl kann zu:* - Ausspähen von Netzwerkinformationen (IP-Adressen), Netzstrukturpläne (Topologie des ITK-Systems) und sonstiger technischer Daten zum Durchführen gezielter Angriffe führen - Verlust von Daten (z.B. aktuelle technische Daten, historische Werte des Leitsystems) führen

3.3.3 Wirkungen von Gefährdungen oder Vorfällen ohne IT-Bezug auf die kDL VvFw

Nachfolgend werden allgemeine Auswirkungen von Störungen im Fernwärmenetz beschrieben, die die Erbringung der kDL VvFw beeinträchtigen können, jedoch keinen Bezug zu informationstechnischen Systemen, Komponenten oder Prozessen haben. Je nach Betreiber und Ausprägung der technischen Lösungen zur Erbringung der kDL VvFw ist individuell zu prüfen, ob ergänzende oder abweichende Maßnahmen getroffen werden müssen.

Störungen und deren Auswirkungen auf die kDL VvFw ohne IT-Bezug sind:

- Versorgungsausfälle oder -einschränkungen durch Störungen bei der Fernwärmeverteilung beispielsweise verursacht durch:
    - zu niedrige Umwälzmenge oder zu niedrige Vorlauf-Temperaturen.
    - zu geringe Wärme im Rohrleitungssystem.
    - Physische Schäden / Störungen an einer Rohrleitung (z.B. durch einen Baggerschaden).
- Versorgungsausfälle oder -einschränkungen durch Störungen an Pumpen/ Pumpstationen beispielsweise verursacht durch:
    - Manipulationen oder mutwillige Beschädigungen von Pumpen.
    - Gefahr durch Überdruck.
    - Personalengpässe bei manuellem Betrieb z.B. im Störungsfall.
    - Extremistische und terroristische Akte.

Durch den Betreiber der kritischen Infrastruktur ist sicherzustellen, dass im Falle von Störungen wirksame Entstörungsprozesse im Unternehmen etabliert sind. Vorteilhaft sind in diesen Situationen große Verbundnetze, wo diese Ereignisse eher auszugleichen sind. Weiter kommt hinzu, dass das Fehlen der kDL erst nach einem längeren Zeitraum nennenswerte Auswirkungen im Zuge deutlicher Raumtemperaturabsenkung (abhängig von der bestehenden thermischen Isolation und Ausführung der Heizungsanlage) hat (mindestens 24 Stunden).

3.3.4 Änderung der allgemeinen Gefährdungslage

Die zu behandelnden IT-relevanten Gefährdungen sind kontinuierlich zu überprüfen und ggf. anzupassen oder zu ergänzen. Dabei müssen insbesondere berücksichtigt werden:

- Allgemeine Gefährdungslage (neu hinzugekommene Angriffsarten oder Angreifer, Neuausrichtung von Angreifern etc.)
- Änderungen der branchenspezifischen Gefährdungslage
- Bekannt gewordene neue Schwachstellen

- Änderungen der Gefährdungslage durch Veränderungen an der Systemarchitektur
- Anderweitige Änderungen an der für die Funktionsfähigkeit der kDL VvFw maßgeblichen ITK oder deren Schnittstellen

Die Überprüfung sollte im Rahmen einer regelmäßigen Neubewertung oder direkt bei Veränderungen oder Anpassungen im Betriebsablauf erfolgen.

3.4 Risikoidentifikation

Im Vorfeld der Risikoanalyse ist eine Risikoidentifikation mit dem Ziel durchzuführen, Risiken aufzufinden, zu erkennen und zu beschreiben, die insbesondere die Informationssicherheit im Zusammenhang mit der kDL VvFw betreffen. Hierzu kann der internationale Standard ISO 31000 in Anwendung gebracht werden.

3.5 Risikoanalyse

Der Zweck einer Risikoanalyse besteht darin, identifizierte Risiken hinsichtlich potenzieller Schadenauswirkungen, wie z.B. „gering“, „mäßig“, „hoch“ und „kritisch“, zu analysieren. Für eine aussagekräftige Risikoanalyse sind geeignete Risikoanalysemethoden und -techniken, z. B. gem. ISO/IEC 27005, ISO 31000 oder BSI-Standard 200-3, anzuwenden.

3.6 Risikobewertung

Für die Abschätzung eines Risikos muss die qualitative/quantitative Eintrittswahrscheinlichkeit der Gefährdungen (siehe Abschnitt 3.3.2) bestimmt werden. Eine anschließende Kombination der Eintrittswahrscheinlichkeit mit den in der BIA ermittelten potenziellen Schadensauswirkungen ergibt für jede Gefährdung dann das Risiko, welches in einer Risikomatrix abgebildet wird.

Folgende Handlungsempfehlungen ergeben sich entsprechend der Einstufung:

- Kritische Risiken, welche eine hohe Eintrittswahrscheinlichkeit in Kombination mit einer signifikanten Schadensauswirkung aufweisen, müssen im Rahmen der Verhältnismäßigkeit zeitnah behandelt und reduziert werden.
- Für Risiken im mittleren Bereich mit moderater Eintrittswahrscheinlichkeit und Schadensauswirkung sind die Behandlungsoptionen hinsichtlich Kosten und Nutzen zu prüfen, und die Risiken je nach Verhältnismäßigkeit zu reduzieren oder zu beseitigen. Eine Übertragung der Risiken darf nur dann stattfinden, wenn von dem betrachteten Risiko keine Auswirkung auf die kDL existiert.
- Unkritische Risiken, deren Eintreten entweder sehr unwahrscheinlich oder deren Schadensauswirkungen gering sind, können toleriert werden oder sind automatisch toleriert. Eine Behandlung kann unter Berücksichtigung von Kosten und Nutzen erfolgen.

Eine Risikoklassifizierung ist im Vorfeld durch das Unternehmen festzulegen und zu begründen.

3.7 Risikobehandlung

Die Risikobehandlung dient dazu, den bewerteten Risiken angemessen zu begegnen. Bspw. sollten kritische Risiken, die für die Erbringung der kDL VvFw bestehen, zeitnah adäquat behandelt werden.

Risiken können auf unterschiedliche Arten behandelt werden, d.h. gemildert oder angenommen werden. Hierzu gehören in Anlehnung z. B. an die ISO 31000 u. a. Risikoreduzierung, Risikobegrenzung, Risikovermeidung, Risikotransfer und Risikoakzeptanz, die in der genannten Reihenfolge auf Anwendung geprüft werden sollten. Hinsichtlich der Risikoakzeptanz beschreibt die Risikotoleranz (Risikoappetit, risk appetite) das Maß der Bereitschaft, individuelle Risiken einzugehen.

4 Maßnahmen zum Umgang mit Risiken

Ergibt sich aus der Bewertung der Risiken ein Handlungsbedarf, das heißt kann ein Risiko nicht toleriert werden, müssen Maßnahmen zur Risikoreduktion abgeleitet werden. Hierfür stehen folgende Optionen zur Verfügung:

1. Risikovermeidung: Durch das Unterlassen von Aktivitäten wird das Risiko vermieden.
2. Risikoreduzierung: Durch geeignete Schutzmaßnahmen wird die Eintrittswahrscheinlichkeit einer Bedrohung reduziert.
3. Risikobegrenzung: Durch geeignete Maßnahmen wird bei Eintritt eines Schadensereignisses der Schaden begrenzt.

Eine eigenständige dauerhafte Risikoakzeptanz relevanter Risiken für die kDL VvFw ist im Sinne des BSIG keine zulässige Option.

4.1 Informationssicherheitsmanagementsystem (ISMS)

Um einen geeigneten Rahmen für die nachhaltige und angemessene Behandlung aller relevanten Risiken und Themenfelder zur Umsetzung der Anforderungen nach § 8a Abs. 1 BSIG zu setzen, ist ein Informationssicherheitsmanagementsystem (ISMS) z.B. in Anlehnung an ISO/IEC 27001, BSI-IT-Grundschutz oder im ICS-Umfeld gemäß IEC 62443 einzuführen und zu betreiben. Mit dem Betrieb des ISMS müssen die in diesem Dokument beschriebenen Vorgehensweisen und Randbedingungen beachtet werden.

Im Rahmen des ISMS muss in Informationssicherheitsrichtlinien und Verfahrensanweisungen der Umgang mit Informationen, Systemen und Software beschrieben und geregelt sein.

Alle Dokumente sind von der Unternehmensleitung bzw. vom jeweiligen Verantwortlichen in Kraft zu setzen und den Beschäftigten sowie relevanten externen Parteien bekannt und zugänglich zu machen. Alle Informationssicherheitsrichtlinien werden in geplanten Abständen oder jeweils nach erheblichen Änderungen überprüft, um sicherzustellen, dass sie nach wie vor geeignet, angemessen und wirksam sind.

Informationssicherheit und deren Weiterentwicklung ist als kontinuierlicher Prozess zu betrachten und folgt im Rahmen des B3S VvFw z.B. dem PDCA-Managementzyklus (Plan/Planen, Do/Durchführen, Check/Überprüfen, Act/Handeln) oder äquivalenten Methoden.

4.2 Asset Management

Im Rahmen des ISMS sind alle, für die kDL VvFW maßgeblichen, informationstechnischen Prozesse, Systeme und Komponenten (Sach- und Informationswerte) zu erfassen, zu dokumentieren und einem Verantwortlichen (Eigner, owner) zuzuordnen.

Weiterhin ist für jedes Asset die Bewertung des Assets in Abhängigkeit seiner Bedeutung für die Erbringung der kDL VvFw zu beschrieben.

Der jeweilige Verantwortliche stellt durch regelmäßige Kontrolle für den verantworteten Sach- oder Informationswert die Aktualität der erfassten Daten im entsprechenden Verzeichnis

sicher, dabei berücksichtigt er auch eventuell vorgenommene Änderungen bis hin zu Außerbetriebnahmen.

Um Daten und Informationen vor unberechtigtem Zugriff oder Ausspähen zu schützen, sind Grundsätze und Regelungen zur Informationsklassifikation und -handhabung zu beschreiben. Alle Informationen, die für den dienstlichen Gebrauch im Unternehmen vorgesehen sind, sei es in mündlicher, schriftlicher, elektronischer oder in anderer Form, müssen gemäß gesetzlicher Anforderungen, ihrer Werte und ihrer Kritikalität entsprechend, vertraulichkeitsklassifiziert und gehandhabt werden. Die Klassifizierung dient dazu, grundlegende Sicherheitsmaßnahmen für den Schutz von Informationen sowie Anweisungen für deren Handhabung festzulegen.

Zum Schutz vor Verlust von Daten sind, unter Beachtung der Informationsklassifizierung und –handhabungsvorgaben, Sicherheitskopien von Informationen, Software und Systemabbildern anzufertigen und regelmäßig auf Gebrauchsfähigkeit zu testen (z.B. in Speicher- und Archivsystemen). Ferner ist darauf zu achten, dass alle Beschäftigten und sonstige (externe) Nutzer von Informationen und informationsverarbeitenden Systemen, diese bei Beendigung ihres Beschäftigungsverhältnisses, ihres Vertrages oder einer sonstigen Vereinbarung an das Unternehmen zurückgeben.

Nicht mehr benötigte Informationen und Datenträger sind entsprechend ihrer Klassifizierung nachhaltig gesichert zu löschen, zu vernichten und/oder zu zerstören. Insbesondere bei Geräten und Betriebsmitteln, die Speichermedien enthalten, ist sicherzustellen, dass jegliche sensiblen Daten vor ihrer Entsorgung oder Wiederverwendung entfernt oder sicher überschrieben worden sind. Die Vernichtung von Papierdokumenten sollte gemäß der DIN Norm 32757-1 oder vergleichbaren Vorschriften erfolgen.

4.3 Vorfallerkennung und -bearbeitung

Um Ausfälle oder Beeinträchtigungen der kDL VvFw aufgrund des Eintretens unvorhergesehener Ereignisse zu verhindern, sind im Rahmen des ISMS geeignete Prozesse zur Vorfallerkennung und -bearbeitung zu definieren. Auf Grundlage der Risikoanalyse und Gefahreneinstufung sind hierzu Maßnahmen zur Gefahrenabwehr sowie zur Auswirkungsminimierung insbesondere in Bezug auf die Detektion von Angriffen und von sonstigen IT-Vorfällen sowie zur Unterscheidung von Angriffen, zur Reaktion auf Angriffe und auf sonstige IT-Vorfälle zu definieren.

Dazu ist es notwendig, geeignete organisatorische, personelle und technische Maßnahmen zu planen, zu implementieren und regelmäßig zu überprüfen. Hierzu zählen beispielsweise:

- Verfahren oder Systeme zur Detektion von Angriffen, Überprüfung des internen Netzwerkverkehrs auf Unregelmäßigkeiten und sonstigen IT-Vorfällen z.B. über den Einsatz von Intrusion Detection Systemen (IDS) oder der Auswertung von Ereignisprotokollen (SIEM-Lösungen)
- Verfahren oder Systeme zur Reaktion auf Angriffe, Sperrung des Zugangs zu bzw. von Geräten beim Auftreten einer Unregelmäßigkeit und sonstigen IT-Vorfällen (siehe Kapitel 4.7.1.6)

- Methoden zur (IT-) Forensik für die Vorfallanalyse zur Beweissicherung, Einschaltung von Behörden und Experten und als Unterstützung zur Schadensbegrenzung sowie der Wiederherstellung der kDL

Weiterhin ist im Rahmen des Vorfallmanagements ein Verfahren zur Analyse von Meldungen über Schwachstellen von Herstellern, staatlichen Stellen und vertrauenswürdigen Dritten zu etablieren, um potenziellen Vorfällen präventiv entgegenzuwirken.

4.4 Notfallmanagement und Übungen

Im Rahmen des ISMS müssen geeignete Prozesse, Verfahren und Maßnahmen zur Aufrechterhaltung der kDL VvFw sowie zur Aufrechterhaltung der Informationssicherheit in Notfallsituationen und (IT-) Krisenlagen etabliert sein.

Die Prozesse des Notfall- und Krisenmanagements müssen in regelmäßigen Abständen überprüft und geübt werden, um ihre Wirksamkeit sowie Umsetzbarkeit in schwierigen Situationen sicherzustellen. Beispiele hierfür können sein:

- Interne Übungen und Systemtests
- Übungen im Rahmen des Notfallmanagements
- Kommunikationsübungen
- Planübungen, Krisenübungen, Training seltener Ereignisse

In allgemeinen Krisensituationen gelten die bilateralen Abstimmungen mit den zuständigen kommunalen Kriseneinrichtungen. Soweit diese nicht bestehen, muss sichergestellt werden, dass die technischen und informationstechnischen Infrastrukturen zumindest in dem Maße geschützt werden, wie es für die Gewährleistung der kDL VvFw notwendig ist.

4.5 Continuity Management für die kDL VvFw

Mit dem Ziel, unter unvorhergesehenen erschwerten Situationen die Aufrechterhaltung der kritischen Dienstleistung und deren Mindestqualität (entsprechend der KRITIS-Schutzziele) gewährleisten zu können, ist das Vorfall- und Notfallmanagement um ein Continuity Management zu ergänzen.

Hierbei sind auf Basis der Risikoanalyse entsprechende Szenarien für die Erstellung sogenannter Business Continuity Pläne (BCP) für die kDL VvFw abzuleiten. Diese BCPs sollten mindestens folgende Punkte enthalten:

- Handlungsanweisungen zu Sofortreaktionen, zum Notbetrieb, zur Wiederherstellung des Leitsystems sowie zum Wiederanlauf (Übergang zum Regelbetrieb)
- Allgemeine Informationen (z.B. referenzierte Dokumente, Test- und Übungspläne)
- Rollen und Verantwortlichkeiten (intern wie extern)
- Notwendige Ressourcen
- Maßnahmen zur Aufrechterhaltung der Informationssicherheit

Für die Koordination des Continuity Managements sollten zudem folgende Aufgaben und Verantwortlichkeiten festgelegt sein:

- Sicherstellung der Verfügbarkeit der BCPs und notwendiger Ressourcen (analog und digital)
- Überprüfung auf Aktualität der BCPs (kontinuierlich)
- Koordination regelmäßiger Tests bzw. Unterweisungen

4.6 Branchenspezifische Technik

Im Gegensatz zur Standard-IT, für deren Absicherung häufig zahlreiche Standard-IT-Sicherheitsmaßnahmen existieren, ist dies für branchenspezifische Technik nicht im gleichen Maße der Fall. Der B3S VvFw geht daher insbesondere auch auf branchenspezifische Informationstechnik und sonstige branchenspezifische Technik ein.

Die Konfiguration und Aktualität der eingesetzten IT-Systeme werden regelmäßig geprüft und mit Sicherheits-Updates und –patches ausgestattet bzw. durch kompensierende IT-Sicherheitsmaßnahmen im OT-Umfeld ausgeglichen, wenn technisch kein zeitnahes Einspielen eines Patches möglich sein sollte.

Bei der Erbringung der kDL VvFw kommt branchenspezifische Technik insbesondere auf den Leitwarten durch spezielle Leittechnik-Software zum Einsatz. Je nach Implementierung sind beispielsweise nachstehende Kommunikationsprotokolle im Einsatz:

- Fernwirkaufgaben seriell (Referenzdokument: IEC 60870-5-101)
- Fernwirkaufgaben TCP/IP (Referenzdokument: IEC 60870-5-104)
- ModBus RTU/ASCII (Referenzdokument: MODBUS over serial line specification and implementation guide V1.02, modbus.org)
- Modbus TCP (Referenzdokumente: IEC 61158/IEC 61784-2)

4.7 Technische Informationssicherheit (Maßnahmenkategorien)

Die beschriebenen Maßnahmen sind nach Schwerpunkten zusammengefasst. Diese stellen in Ihrer Form keine Wertung dar. Sie sind soweit anzuwenden, sofern ihre Wirksamkeit für die Erbringung der kDL relevant sind und wie es im Umgang mit Gefährdungen sinnvoll und verhältnismäßig ist.

Nachfolgende Maßnahmen sind für die Absicherung der technischen Systeme in der KRITIS-Umgebung geeignet. Ihr Einsatz erfolgt bei Erfordernis auf Basis einer individuellen Risikobewertung.

4.7.1 Absicherung von Netzwerkübergängen (OT-Infrastruktur/Zonenübergänge)

4.7.1.1 Inventarisierung aller Netzzugänge

Alle stationären und mobilen OT-Netzwerkzugänge sind zu inventarisieren, um den Zugriff auf Unternehmensressourcen zu steuern. Bei der Inventarisierung sind insbesondere Firewall-Regeln mit Ports und erlaubten IP-Adressen sowie Zugänge zu Terminalservern zu berücksichtigen.

Eine mögliche Implementierungshilfe für die Maßnahme findet sich in

- [VGB S-175]: 2.5.4 Inventarisierung und Kennzeichnung
- [ISO/IEC 27001]: A.13.1.1 Netzwerksteuerungsmaßnahmen

4.7.1.2 Netzwerktrennung und Segmentierung, besonders im ICS-Umfeld

Der Einfluss von IT-Störungen auf die für die Funktionsfähigkeit der kDL VvFw maßgeblichen Prozesse soll durch eine geeignete Wahl der Architektur reduziert werden, also durch eine robuste bzw. resiliente Architektur. Geeignet hierfür wäre eine Architektur, welche mithilfe einer Netzwerksegmentierung die informationstechnischen Systeme, Komponenten oder Prozesse in Abhängigkeit ihrer Kritikalität in Zonen aufteilt und die Kommunikation untereinander über spezifische Prozesse reglementiert (Zonenmodell, siehe Abbildung 2).

Zur Minimierung von Fehlfunktionen der IT, die sowohl vorsätzlich als auch nicht-vorsätzlich ausgelöst werden können, ist zweckmäßiger Weise eine Architektur zu verwenden, die eine Trennung der kritischen Systeme zur Anlagensteuerung von anderen Systemen und dem Extranet (Internet) vorsieht. Der Zugriff auf die kritischen Systeme findet über gesicherte Zugänge (Security Gateways) statt.

Eine physikalische oder logische Trennung der Netzwerke muss stattfinden, um nur erlaubte Dienste und Kommunikation im Netzwerk zur Verfügung zu stellen. Der nicht erlaubte Einsatz von Diensten oder unerwünschte Kommunikation wird verhindert bzw. blockiert.

Die Architektur eines geeigneten Zonenmodells kann für eine adäquate Umsetzung wie folgt gestaltet sein. Hierbei kann für einige Betreiber der Einsatz von speziell abgesicherten Sonderzonen relevant sein:

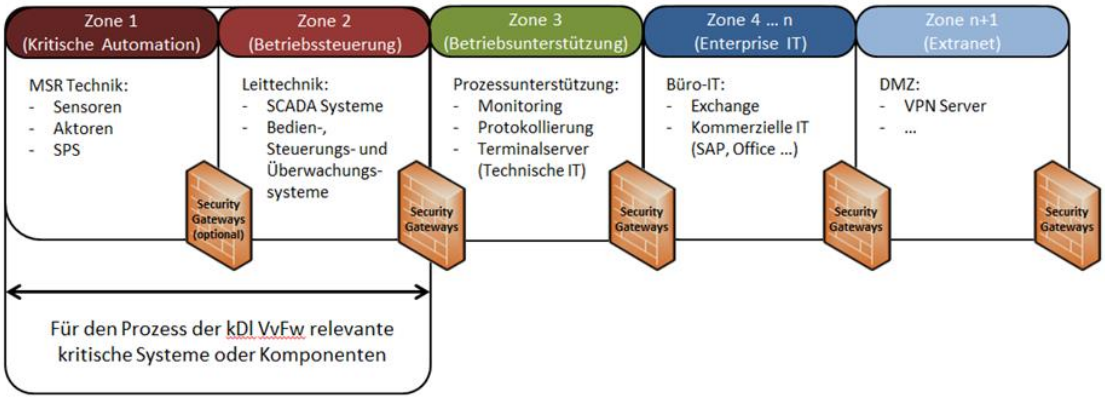

Abbildung 2: Architektur Zonenmodell

Mit folgenden Prinzipien sollte die IT-Architektur gegen vorsätzlich oder unbeabsichtigt herbeigeführte Fehlfunktionen geschützt werden:

- “Prinzip der geringsten Rechtevergabe” (least privilege principle) – Nutzer und Systemkomponenten haben nur die erforderlichen Privilegien und Zugriffsrechte, um ihre Aufgaben und Funktionen zu erfüllen.
- “Prinzip der Verteidigung in der Tiefe” (defence in depth principle) – Sicherheitsbedrohungen werden nicht nur durch eine Einzelmaßnahme, sondern durch verschiedene sich ergänzende, d.h. komplementäre, Sicherheitstechniken auf verschiedenen Systemebenen gemildert.
- “Prinzip der Redundanz” (redundancy principle) – Mithilfe eines geeigneten redundanten Systemdesigns sollen Fehlfunktionen einzelner informationstechnischer Komponenten kompensiert werden.
- “Prinzip von Schutz, Erkennung, Maßnahmen” (protection, detection, response principle) – Es werden Maßnahmen (controls) mit dem Ziel implementiert, hinsichtlich Sicherheitsereignissen den Schutz zu erhöhen, ihre Erkennung zu verbessern sowie die Maßnahmen für eine Reaktion zu erhöhen.
- “Prinzip des Vertrauens in Zonen” (zone model trust principle) – Eine Zone x vertraut nicht ohne generelle Sicherheitsmaßnahmen einer Zone x+1. D.h., dass sich beispielsweise ein Nutzer bzw. eine Systemkomponente in einer Zone x+1 vor dem Zugriff auf eine Ressource in der Zone x zuvor bei dieser authentifizieren muss.

Für Betreiber mit spezifischen Komponentenanforderungen sollte das „Prinzip der gesicherten Subzonen“ (secured subzones principle) in Schichten (layers) nebst Separationsstufen (separation levels) zur Anwendung gebracht werden:

- Zur zielgerichteten Anwendung des Prinzips der gesicherten Subzonen für Komponenten und Systeme ist es erforderlich, eine feinere Untergliederung der Primärzonen OT und IT in Schichten durchzuführen (siehe **Fehler! Verweisquelle konnte nicht gefunden**

werden.) sowie zusätzliche DMZ für die Primärzonen OT und IT für Kommunikationsverbindungen einzurichten. Subzonen sind logisch oder/und physikalisch segmentierte Komponenten oder Systeme, die einen Perimeterschutz haben, d.h. der Perimeter wird überwacht (monitoring) und kontrolliert (controlling). Den Subzonen werden in Abhängigkeit ihrer (Nicht-)Kritikalität zur Erbringung der kDL VvFw Separationsstufen (separation levels) zugeordnet. Die Höhe der Separationsstufen bestimmt die anzuwendenden zusätzlichen Sicherheitsmaßnahmen wie bspw. zur Segmentierung, Kommunikation und Authentisierung.

Beispielsweise könnten auf diese Weise Sensoren in einer Subzone in Schicht 0 mit externer Verbindung eingesetzt werden, die für die Erbringung der kDL VvFw unerheblich sind. Diese Subzone wäre über entsprechende Sicherheitsmaßnahmen hinsichtlich ihres Perimeters von anderen Subzonen strikt getrennt, d. h. die Kommunikation mit anderen Subzonen in der OT-Primärzone wird überwacht und unterbunden. Zudem würde sie aufgrund ihrer bspw. mittleren Kritikalität, da sie nur für einen speziellen Dienstleister zur Verfügung steht, entsprechende zusätzliche Schutzmaßnahmen erhalten. Für die Kommunikation mit der externen Stelle wird eine OT DMZ-Instanz erzeugt, die ihrerseits eine Separationsstufen erhält, um die Schutzmaßnahmen bspw. hinsichtlich der Authentisierung und Verschlüsselungsstärke der Kommunikationsverbindung festzulegen.

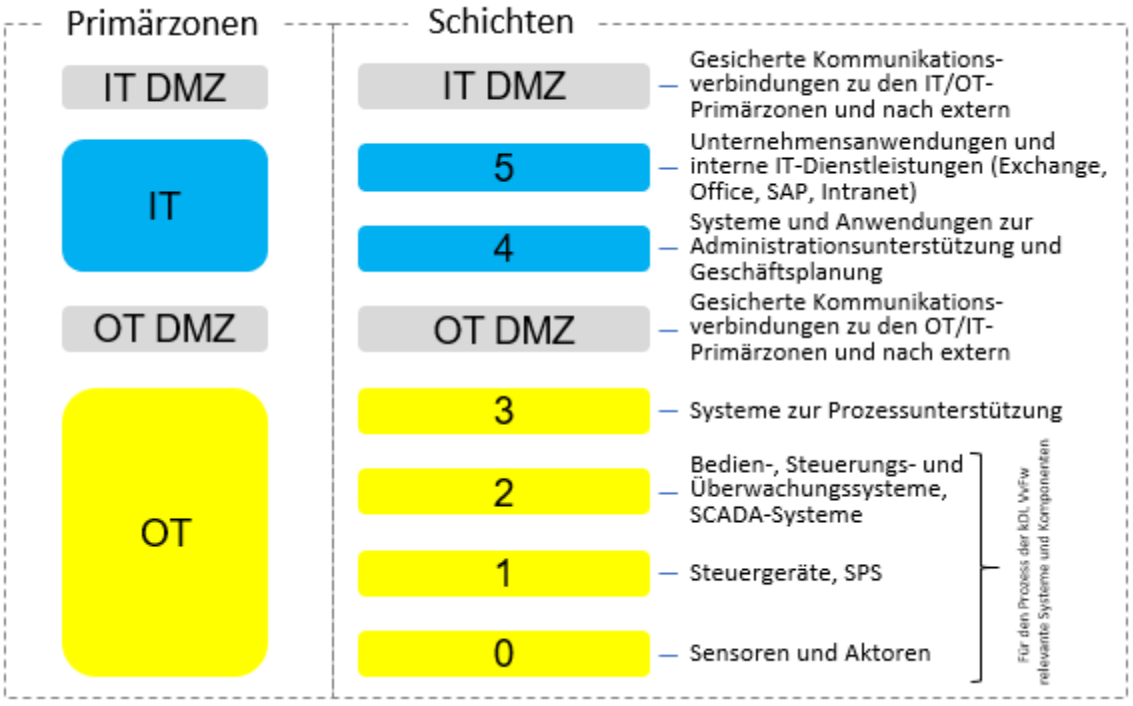

Abbildung 3: Zonenmodell untergliedert in Schichten zur Erweiterung um Subzonen

Eine mögliche Implementierungshilfe für die Maßnahme findet sich in:

- [VGB S-175]: 2.3.1.1 Netzwerksegmentierung

- [ISO/IEC 27001]: A 13.1.3 Trennung in Netzwerken

4.7.1.3 Absicherung der Fernzugriffe, Remote Access

Beim Einsatz von Fernzugriffen ist eine Absicherung durch technische Zugangskontrollen, die den Fernzugang bei kritischen Komponenten freigeben, steuern und überwachen, einzusetzen. Der Einsatz einer Zweifaktor-Authentifizierung ist grundsätzlich erforderlich.

Systeme, die den Zugriff aus dem Extranet auf das interne Netzwerk regeln, sollten auf dem aktuellen Stand der Technik sein und regelmäßig auf ihre Wirksamkeit und Verlässlichkeit überprüft werden. Etwaig übertragene Dateien im Rahmen einer Fernwartung (z.B. Sicherheitsupdates) sollten zusätzlich auf Schadcode geprüft werden. Der Verbindungsaufbau sollte protokolliert und die Sitzung idealerweise aufgezeichnet werden.

Eine mögliche Implementierungshilfe für die Maßnahme findet sich in:

- [VGB S-175]: 2.3.1.3 Fernzugriffe
- [ISO/IEC 27001]: A 6.2.2 Telearbeit

4.7.1.4 Sicherheitsgateways, Firewalls

Sicherheitsgateways sind typischerweise Firewalls, Proxyserver, (VPN-) Router und Switches.
Firewalls bilden einen elementaren Baustein beim Aufbau von Subnetzen oder Demilitarisierten Zonen (DMZ). Beim Betrieb einer Firewall sollten folgende Punkte beachtet werden:

- Die Definition der Filterregeln ist so restriktiv wie erforderlich zu gestalten, so dass nur die erforderlichen Zugriffe erlaubt sind.
- Eine Überprüfung der Einstellungen muss regelmäßig erfolgen.
- Nicht benötigte Ports müssen gesperrt werden.
- Es sollte immer eine aktuelle Firmware-Version installiert sein und auch benutzt werden.
- Patches sollten umgehend nach Bekanntgabe von Sicherheitslücken getestet und eingespielt werden.
- Sicherheitsrelevante Ereignisse und Änderungen an der Konfiguration bzw. den Filterregeln sollten protokolliert und regelmäßig ausgewertet werden.

Eine mögliche Implementierungshilfe für die Maßnahme findet sich in:

- [VGB S-175]: 2.3.1.2 Sicherheitsgateway (Firewall)
- [ISO/IEC 27001]: A 13.1.2 Sicherheit von Netzwerkdiensten

4.7.1.5 Härtung und sichere Basiskonfigurationen

Im Rahmen der Härtung werden in einzelnen IT-Systemen oder in der gesamten Netzwerkumgebung verschiedene Maßnahmen zur nachhaltigen Erhöhung der IT-Sicherheit umgesetzt.
Generell sollte jede IT-Komponente vor ihrem Einsatz folgender Härtung unterzogen bzw. die Basiskonfiguration wie folgt angepasst werden:

- Deaktivierung aller nicht benötigen Funktionen / Dienste
- Änderung oder Deaktivierung aller System-Accounts
- Deaktivierung evtl. vorhandener Gastzugänge
- Aktualisierung der Version (Software, Hardware)
- Aktivierung der Protokollierung aller relevanten Statusmeldungen
- Umleitung der Protokollmeldung zu einem zentralen Log-Server, falls möglich.

Härtungsmaßnahmen ergeben sich aus dem Einsatzzweck der Komponente und den technischen Konfigurationsmöglichkeiten und müssen im Einzelfall festgelegt werden.

Eine mögliche Implementierungshilfe für die Maßnahme findet sich in:

- [VGB S-175]: 2.3.2.3 Härtungsmaßnahmen
- [ISO/IEC 27001]: A 13.1.1 Netzwerksteuerungsmaßnahmen

4.7.1.6 Schnittstellenkontrolle, Intrusion Detection/Prevention Systeme (IDS, IPS)

Um Angriffsversuche frühzeitig zu erkennen und darauf zu reagieren, sollten Intrusion Detection Systeme (IDS) und falls technisch umsetzbar Intrusion Prevention Systeme (IPS) eingesetzt werden, sodass der IT-Betrieb frühzeitig alarmiert (IDS) oder bereits eine automatisierte Reaktion auf einen Angriff (IPS) eingeleitet werden kann.

Eine mögliche Implementierungshilfe für die Maßnahme findet sich in:

- [VGB-S 175] 2.3.2.9 Host Intrusion Detection/Prevention
- [ISO/IEC 27001]: A 13.1.2 Sicherheit von Netzwerkdiensten

4.7.1.7 Absicherung mobiler Netzwerkzugänge, mobile Sicherheit, Telearbeit, ggf. BYOD

Mobile Endgeräte (z.B. Smartphone, Tablets) stellen hinsichtlich ihrer Rechenleistung und Konnektivität eine potenzielle Bedrohung dar, wenn sie direkt mit OT-Komponenten verbunden werden, um gezielte Angriffe auf Anlagen der kritischen Infrastruktur durchzuführen.

Aufgrund ihrer Mobilität eignen sie sich besonders gut, um Daten von außen in die Zonen 1-3 bzw. in die OT-Primärzone einzuschleusen und somit technisch das Zonenmodell zu umgehen.

Darüber hinaus verfügen die Geräte in der Regel über einen separaten Internetzugang per Mobilnetz und somit über die Möglichkeit, eine Brücke aus dem Internet direkt in die Kritische Infrastruktur zu bauen.

Aus diesem Grund sollten Smartphones, Tablets und andere Mobilgeräte für die dedizierte Anwendung im OT-Netzwerk nur dann mit diesem verbunden werden, wenn sie keine Verbindung in ein anderes Netz aufbauen können.

Ist der Einsatz mobiler Geräte unumgänglich (z.B. bei der Wartung oder Diagnose), so sind diese Geräte angemessen abzusichern.

Für Arbeiten mit mobilen Wartungsgeräten ist festzulegen, welche Arbeiten auszuführen sind und sicherzustellen, dass die eingesetzten Mitarbeiter die entsprechende Qualifikation haben. Darüber hinaus sind, wo erforderlich, geeignete technische Sicherungsmaßnahmen und organisatorische Maßnahmen (z.B. Vier-Augen-Prinzip) anzuwenden.

Bei Arbeiten an Anlagen mit hohem Schutzbedarf wird zudem empfohlen, die Zusatzmaßnahmen auf alle abhängigen Systeme auszuweiten, um sicherzustellen, dass es zu keinen unbeabsichtigten Änderungen auf Anlagen kommt, die in Abhängigkeit mit der betroffenen Anlage stehen (z. B. durch Probeläufe oder geeignete Testmaßnahmen).

Über organisatorische Maßnahmen ist sicherzustellen, dass auf mobilen Geräten, die z.B. für die Telearbeit oder Wartung genutzt werden, ausschließlich Software installiert ist, die für den Arbeitszweck erforderlich ist.

Darüber hinaus sollte eine Systemhärtung durchgeführt werden und es muss gewährleistet sein, dass die Geräte regelmäßig gepatcht und auf Malware (Schadprogramme) untersucht werden.

Das Einbinden von BYOD in eine KRITIS-Umgebung ist zu vermeiden, da die Sicherheit dieser Geräte nicht ausreichend garantiert werden kann.

Eine mögliche Implementierungshilfe für die Maßnahme findet sich in:

- [VGB S-175]: 2.3.2.4 Umgang mit Wechseldatenträgern/mobilen Geräten
- [ISO/IEC 27001]: A.6.2.1 Richtlinie zu Mobilgeräten

4.7.1.8 DDoS-Mitigation

DDoS-Angriffe zielen auf die Beeinträchtigung der Verfügbarkeit von Komponenten ab. Um die Gefahr eines DDoS-Angriffs zu minimieren bzw. den Angriff zu erschweren sollten folgende Gegenmaßnahmen getroffen werden:

- On Premises
  Betrieb einer entsprechenden technischen Gegenmaßnahme am Standort.
- Content Delivery Network
  Hierbei wird der Netzwerkverkehr in ein spezielles Netzwerk geleitet, wo er von mehreren Servern beantwortet wird, die alle den gleichen Inhalt besitzen.
- DDoS-Mitigation als Service
  Hierbei wird der gesamte Netzwerkverkehr über das Internet zu einem Dienstleister geschickt, der den Inhalt vorher auf Unregelmäßigkeiten überprüft und ihn dann an den Empfänger weiterleitet.

Durch den Einsatz eines Zonenmodells, wie unter 4.7.1.2 beschrieben, kann dieser Gefährdung effektiv begegnet werden. Anwendungen, die vor DDOS-Angriffen geschützt werden sollen, können hierfür in den Zonen 1-3 bzw. der OT-Primärzone betrieben werden.

Eine mögliche Implementierungshilfe für die Maßnahme findet sich in:

- [ISO/IEC 27001]: A 13.2.3 elektronische Nachrichtenübermittlung

4.7.1.9 Network Access Control (NAC)

NAC-Lösungen sollten insbesondere zur Bestandsaufnahme im Rahmen des Asset-Managements eingesetzt werden. Das NAC schützt das Netzwerk vor dem Eindringen unerwünschter Geräte und verschafft eine Übersicht aller Geräte im Netzwerk. Darüber hinaus bieten einige NAC-Lösungen eine zentrale Administration der Netzwerkkomponenten, mit der Option den Netzwerkzugang nur Geräten mit aktuellem Softwarestand zu erlauben.

Durch den Einsatz eines Zonenmodells, wie unter 4.7.1.2 beschrieben, kann das unbemerkte Einbinden fremder Geräte in das Netzwerk unterbunden werden.

Eine mögliche Implementierungshilfe für die Maßnahme findet sich in:

- [ISO/IEC 27001]: A.9.1.2 Zugang zu Netzwerken und Netzwerkdiensten

4.7.1.10 Router, VPN-Gateway

Es gelten die gleichen Bedingungen wie im Abschnitt 4.7.1.4.

Zusätzlich besteht für VPN-Zugänge die Vorgabe, eine Verschlüsselung nach dem Stand der Technik zu verwenden und die Notwendigkeit, ein Life-Cycle-Management für die VPN-Benutzer zu etablieren.

Eine mögliche Implementierungshilfe für die Maßnahme findet sich in:

- [VGB S-175]: 2.3.1.2 Sicherheitsgateway (Firewall)
- [ISO/IEC 27001]: A 13.1.2 Sicherheit von Netzwerkdiensten

4.7.2 Sichere Interaktion im Internet

4.7.2.1 Browser-Virtualisierung, Exploit Protection

Um die Gefahren eines Sicherheitsvorfalls durch eine Softwareschwachstelle zu minimieren, wird der Einsatz von virtualisierten Browsern empfohlen.

Der virtualisierte Browser hat nicht nur den Vorteil, dass das darunterliegende System stärker gehärtet werden kann, sondern auch, dass eine potenzielle Infektion nur das virtuelle System infizieren würde.

Durch den Einsatz eines Zonenmodells wie unter 4.7.1.2 beschrieben kann dem Schaden durch Exploits effektiv begegnet werden.

Eine mögliche Implementierungshilfe für die Maßnahme findet sich in:

- [VGB S-175]: 2.3.2.8 Einsatz von Virtualisierungstechnologien
- [ISO/IEC 27001]: A 12.2.1 Maßnahme gegen Schadsoftware

4.7.2.2 Web-Filter

Die Verwendung eines Application Level Gateways (ALG) mit entsprechender Web-Filter-Funktion erlaubt, den Datenverkehr zwischen zwei Netzwerken oder auch Systemen zu prüfen und ggf. zu unterbinden. Üblicherweise sind Webfilter ein Bestandteil gängiger Proxy-Server- oder Firewall-Lösungen.

Einen besonderen Stellenwert haben die ALGs im KRITIS-Bereich beim Betrieb des Zonenmodells und sollten daher dort zum Einsatz kommen. Hier wird der Übergang von einer in die nächste Zone mit Hilfe von Firewalls abgesichert.

Eine mögliche Implementierungshilfe für die Maßnahme findet sich in:

- [ISO/IEC 27001]: A 13.1.3 Trennung in Netzwerken

4.7.2.3 Virtuelle Schleuse

Eine Virtuelle Schleuse bezeichnet die technische Möglichkeit, Funktionen, die für den Unternehmensbereich als zu riskant in der Produktivumgebung erachtet werden, durch virtualisierte Instanzen zur Verfügung zu stellen.

Sollte es in dieser Konstellation zu Sicherheitsvorfällen kommen, bleibt die Produktivumgebung davon unberührt.

Mögliche Einsatzszenarien für virtuelle Schleusen sind überall dort, wo keine Daten von außen bzw. keine ungeprüften Daten in die Produktivumgebung fließen sollen, wie z.B. USB-Schleusen, Internet-Schleusen oder auch Medien-Schleusen. Die virtuellen Schleusen sollten zielgerichtet Benutzern, die externe Daten aus nicht vertrauenswürdigen Quellen verarbeiten, zur Verfügung gestellt werden.

Eine mögliche Implementierungshilfe für die Maßnahme findet sich in:

- [ISO/IEC 27001]: A 12.2.1 Maßnahme gegen Schadsoftware

4.7.2.4 Sichere Dokumentenerstellung

Es soll ein System zur sicheren Dokumentenerstellung für alle Managementdokumente und Dokumente, die für den Betrieb und die Sicherheit der Systeme relevant sind, eingesetzt werden. Der Verantwortliche für ein Dokument, zumeist der Autor, sowie das Datum, ab wann das Dokument Gültigkeit bzw. welche Versionsnummer es besitzt, müssen immer eindeutig und zweifelsfrei erkennbar sein. Weitere Kriterien von Dokumenten wären bspw. die Versionierung und die Vertraulichkeitsklassifizierung. Veränderungen an den Dokumenten sollen nachvollziehbar sein.

Eine mögliche Implementierungshilfe für die Maßnahme findet sich in:

- [VGB S-175]: 2.5 Dokumentation

4.7.2.5 Detektionswerkzeuge für gezielte Angriffe auf Webseiten bzw. E-Mails

Detektionswerkzeuge dienen dem Einsatz zur Angriffserkennung auf Webseiten und E-Mails. Im Fokus dieser Maßnahme steht die Absicherung von Web-Servern und Mail-Servern gegen Kompromittierung und der unberechtigten Veränderung der Inhalte.

Es sollte zudem ein Zonenmodell wie unter 4.7.1.2 beschrieben zum Einsatz kommen, damit die Web- und Mail-Server nur in den Zonen 4-6 (Office-IT) bzw. der IT-Primärzone eingesetzt werden können und damit getrennt und ohne direkte Verbindung zu den Zonen 1-3 bzw. der OT-Primärzone betrieben werden.

Eine mögliche Implementierungshilfe für die Maßnahme findet sich in:

- [ISO/IEC 27001]: A 12.2.1 1 Maßnahme gegen Schadsoftware

4.7.2.6 Security Information and Event Management (SIEM)

Angriffsversuche und auch die Vorbereitung eines Angriffs hinterlassen Spuren. Um diese Angriffe zu detektieren, ist es erforderlich, die Log-Informationen der einzelnen Anwendungen und Systeme zentral zu sammeln und auszuwerten.

Ein SIEM durchsucht die Log-Einträge nach Mustern, die auf einen möglichen Angriff hindeuten. Die Effektivität des SIEM-Systems kann durch eine Echtzeitanalyse weiter erhöht werden.

SIEM-Systeme sollten die Log-Informationen aller relevanten Systeme analysieren.

Eine mögliche Implementierungshilfe für die Maßnahme findet sich in:

- [ISO/IEC 27001]: A 12.4.1 Ereignisprotokollierung

4.7.3 Sichere Software

4.7.3.1 Spam-Abwehr, Content Filtering

Zur Abwehr von Spam, Meldung von potenziellen Phishing-Angriffen und der Früherkennung von Infektionen einzelner Postfächer empfiehlt sich der Einsatz eines eigenen Mail-Servers mit entsprechenden Sicherheitsfunktionen.

Wichtig für die Wirksamkeit des Filters ist die kontinuierliche Versorgung mit Updates seitens der Hersteller.

Es sollte zudem ein Zonenmodell wie unter 4.7.1.2 beschrieben zum Einsatz kommen, damit die Mail-Server nur in den Zonen 4-6 (Office-IT) bzw. der IT-Primärzone eingesetzt werden können und damit getrennt und ohne direkte Verbindung zu den Zonen 1-3 bzw. der OT-Primärzone betrieben werden.

Eine mögliche Implementierungshilfe für die Maßnahme findet sich in:

- [ISO/IEC 27001]: A 12.2.1 Maßnahme gegen Schadsoftware

4.7.3.2 Toolunterstützte Inventarisierung von Hardware und Software

Um eine fortlaufende Inventarisierung aller IT-Systeme im Rahmen einer Configuration Management Database (CMDB) zu ermöglichen, bedarf es einer entsprechenden Tool-Unterstützung. Auf diese Weise kann schnell ermittelt werden, ob und welche Systeme von aktuellen Hard- oder Softwareschwachstellen betroffen sind.

Mit Hilfe dieser Form der Inventarisierung kann ggfs. sogar eine automatisierte Schwachstellenerkennung einhergehen, wenn die in den Schwachstellenmeldungen genannten Assets automatisiert mit dem Inventar abgeglichen werden.
Beim Betrieb eines Zonenmodells, wie in 4.7.1.2 beschrieben, ist der Einsatz des Systems in den Zonen 4-6 bzw. der IT-Primärzone unproblematisch. In den Zonen 1-3 bzw. der OT-Primärzone hingegen ist der Informationsaustausch zwischen der zu prüfenden Zone und dem System, dass die Prüfung ausführt, nicht zulässig.

Daher sollte ein hybrider Ansatz mit einer automatisierten Erfassung für die Systeme und Komponenten in den Zonen 4-6 bzw. der IT-Primärzone und einer manuellen Erfassung für die Systeme und Komponenten der Zonen 1-3 bzw. der OT-Primärzone zum Einsatz kommen.

Eine mögliche Implementierungshilfe für die Maßnahme findet sich in:

- [ISO/IEC 27001]: A 8.1.1 Inventarisierung der Werte

4.7.3.3 Zentrales Patch- und Änderungsmanagement (Change Management), Konfigurationsmanagement

Um Schwachstellen wirksam vorzubeugen ist es zweckmäßig, dass die eingesetzte Software auf dem aktuellen Stand ist. Im Rahmen des Änderungsmanagements wird gewährleistet, dass die Änderungen an den Systemen in dieser Form beabsichtigt sind und auch keine negativen Auswirkungen auf andere Systeme haben. Jede Veränderung an einem System folgt fest vorgegebenen Prozessen des Änderungsmanagements.

Um dies zu bewerkstelligen, sollte für Updates und Patches vorzugweise eine zentrale Verwaltungslösung eingesetzt werden. Bevor Aktualisierungen eingespielt werden, sollen diese vorher getestet und im Rahmen eines Änderungsmanagements freigegeben werden.

Beim Betrieb eines Zonenmodells, wie in 4.7.1.2 beschrieben, ist der Einsatz eines zentralen zonenübergreifenden Konfigurationsmanagements nicht möglich, daher sollte ein hybrider Ansatz mit einer zentralen Konfiguration für die Systeme und Komponenten in den Zonen 4-6 bzw. der IT-Primärzone und einer manuellen Konfiguration für die Systeme und Komponenten der Zonen 1-3 bzw. der OT-Primärzone zum Einsatz kommen.

Ein Änderungsmanagement kann bspw. zudem folgende Aspekte umfassen:

- Änderungen an Systemen, Hardware oder Software werden dokumentiert.
- Darüber hinaus wird vor Änderungen an Betriebsplattformen eine Risikoanalyse durchgeführt und entsprechende Maßnahmen ergriffen, um sicherzustellen, dass es keine negativen Auswirkungen auf die kDL VvFw gibt.
- Für neue Informationssysteme, Aktualisierungen und neue Versionen sind Abnahmetests und dazugehörige Kriterien festzulegen.
- Änderungen an Systemen, Hardware oder Software sind auf ein Mindestmaß zu beschränken und vor der Durchführung auf Erfordernis und Alternativen zu prüfen.

Eine mögliche Implementierungshilfe für die Maßnahme findet sich in:

- [VGB S-175]: 2.3.3.1 Patchmanagement

- [ISO/IEC 27001]: A 12.1.2 Änderungssteuerung

4.7.3.4 Schutz vor Schadsoftware

Es ist eine aktuelle Malwareschutz-Lösung auf Clients für Büroarbeitsplätze einzusetzen sowie entsprechende Webfilter, die unerwünschte Inhalte blockieren. Idealerweise handelt es sich hierbei um eine Client-Server-Lösung mit der die Signaturen der Schadsoftware zentral verteilt, die flächendecke Verteilung geprüft und eine zentrale Quarantänezone definiert werden kann. Darüber hinaus können Malwarevorfälle schneller identifiziert und behandelt werden.
Für den OT-Bereich ist es insbesondere wichtig und erforderlich, dass eingebrachte Software (Updates, Patches) zuvor mit aktuellen Malwarescannern geprüft wird.

Eine mögliche Implementierungshilfe für die Maßnahme findet sich in:

- [ISO/IEC 27001]: A 12.2.1 Maßnahme gegen Schadsoftware

4.7.3.5 Softwaretest und Freigabe

Sichere Software setzt vor ihrem erstmaligen Einsatz voraus, dass ein Verfahren implementiert ist, um sie vor der Produktivsetzung auf Fehler zu testen. Erst nach erfolgreichem Test kann eine Freigabe erfolgen. Bei einer Weiterentwicklung der Software für Bereiche, die Auswirkungen auf die Kritische Infrastruktur haben könnten, ist ein erneuter Test durchzuführen.

Um zu vermeiden, dass fehlerhafte Software, Firmware oder Hardware ins Unternehmen eingebracht und verwendet werden kann, sind im Rahmen des ISMS:

- Generelle Regeln für Administratoren zur Installation von Software festzulegen und umzusetzen
- Verfahrensweisen zur Steuerung von Softwareinstallationen auf sich im Betrieb befindenden Systemen zu definieren und zu implementieren.

Eine mögliche Implementierungshilfe für die Maßnahme findet sich in:

- [VGB S-175]: 2.2.7 Funktionstest, Inbetriebnahme und Abnahme
- [ISO/IEC 27001]: A 12.5.1 Installation von Software auf Systemen im Betrieb

4.7.3.6 Software Development Security (sichere Softwareentwicklung)

Der Betrieb sicherer Software setzt voraus, dass Softwareentwicklung auf Basis klar definierter Vorgehensweisen erfolgt. Der Aufwand Sicherheitslücken von Beginn an zu verhindern ist gemessen an dem Aufwand Fehler im fertigen

Produkt zu finden und zu korrigieren um ein Vielfaches geringer.

Daher sollte eine Verfahrensanweisung in Kraft gesetzt werden, die regelt wie die sichere Softwareentwicklung zu erfolgen hat. Hierzu gehören bspw. die programmiertechnische Vermeidung von Schwachstellen wie SQL-Injections, Buffer-Overflows, Cross Site Scripting usw. und Softwareverifikation.

Eine mögliche Implementierungshilfe für die Maßnahme findet sich in:

- [VGB S-175]: 2.2.6.4 Entwicklung
- [ISO/IEC 27002:2013]: A 14.2 Sicherheit in Entwicklungs- und Unterstützungsprozessen

4.7.3.7 Security Operations

Es müssen Prozesse zur Überwachung eines sicheren Betriebs mit einem regelmäßigen Reporting etabliert werden.
Daher wird der Einsatz eines Security Operations Center (SOC) empfohlen, das eingehende Schwachstellenmeldungen zentral mit der Asset-Liste vergleicht, um möglichst schnell auf Schwachstellen, die das Unternehmen betreffen, adäquat reagieren zu können. Dabei ist zu beachten, dass auch der Hersteller vertraglich in das Prozedere einzubinden ist, um eine gesamtheitliche Unterstützung zu gewährleisten und Ausfallzeiten zu minimieren.

Eine mögliche Implementierungshilfe für die Maßnahme findet sich in:

- [ISO/IEC 27001]: A 12.1.1 Dokumentierte Betriebsabläufe

4.7.3.8 Sichere Beschaffung und Aussonderung (sicheres Löschen, Überwachung, Datensicherung und -wiederherstellung (Backup & Recovery), Archivierung)

Hard- und Softwarekomponenten, die das Ende des Produkt-Lebenszyklus erreicht haben und vom Hersteller nicht mehr unterstützt werden, führen zu einem erhöhten Betriebsrisiko. Neue Schwachstellen werden in der Regel seitens der Hersteller nicht mehr geschlossen.

Daher hat eine Sicherheitsbetrachtung der einzelnen Komponenten zu erfolgen und es sind in Abhängigkeit von der Bedeutung der Komponente für die Produktion entsprechende Sicherheitsmaßnahmen zu identifizieren und zu implementieren.

Es sollte eine Verfahrensanweisung in Kraft gesetzt werden, die den gesamten Lebenszyklus von Hard- und Softwarekomponenten von der Beschaffung/Entwicklung über die Betriebsdauer bis hin zur Dekomissionierung der Komponenten beschreibt. Zudem sollten für die Betriebsdauer der Komponenten Prozeduren etabliert werden, die u.a. das sichere Löschen von Daten, die Datensicherung/-wiederherstellung und Datenarchivierung festlegen.

Eine mögliche Implementierungshilfe für die Maßnahme findet sich in:

- [VGB S-175]: 2.3.3.2 Datensicherungskonzept (Backup)
- [ISO/IEC 27001]: A 8.3.2 Entsorgung von Datenträgern

4.7.4 Sichere Authentisierung

4.7.4.1 Identitäts- und Rechtemanagement

Der Zugriff auf Informationen und informationsverarbeitende Systeme ist auf das nötige Maß zu beschränken und aktiv über ein Benutzer- und Zugriffsrechtemanagement zu verwalten und regelmäßig zu überprüfen. Es muss sichergestellt sein, dass Benutzer ausschließlich Zugriff auf diejenigen Systeme und Netzwerke haben, zu deren Nutzung sie ausdrücklich befugt und berechtigt sind, zum Beispiel durch eine authentifizierte Anmeldung an Systemen mit Nutzernamen und einem Passwort mit geeigneter Stärke. Beantragte Berechtigungen sollten vor Vergabe adäquat geprüft werden. Hierbei ist es zweckmäßig, dass die Antragsprüfung durch den jeweiligen Vorgesetzten und durch bspw. dem jeweiligen Anwendungs- oder Systemverantwortlichen erfolgt.

Um die Möglichkeit zu unterbinden, unbefugt Änderungen an Berechtigungen vorzunehmen, sollten nur Administratoren gemäß der Vorgaben in 4.7.4.4 solche Änderungen vornehmen.

Eine mögliche Implementierungshilfe für die Maßnahme findet sich in:

- [VGB S-175]: 2.3.2.1 Authentisierung
- [ISO/IEC 27001]: A 6.1.2 Aufgabentrennung

4.7.4.2 Multifaktor-Authentisierung

Die Multifaktor-Authentisierung dient der Erhöhung des Schutzes eines Logons vor Kompromittierung. Dieses ist insbesondere für administrative und Remotezugänge relevant.

In Bereichen, die als besonders kritisch eingestuft worden sind, sollte mindestens eine Zwei-Faktor-Authentisierung eingesetzt werden, um die Zuverlässigkeit der Identitätsbestimmung zu erhöhen. Hierbei sollten unterschiedliche Merkmalsklassen (Wissen, Besitz, Biometrisches Merkmal, Ort/Zeit) kombiniert werden.

Eine mögliche Implementierungshilfe für die Maßnahme findet sich in:

- [VGB S-175]: 2.3.2.1 Authentisierung
- [ISO/IEC 27001]: A 9.4.2 sichere Anmeldeverfahren

4.7.4.3 Zugriffskontrolle (Sicheres Logon)

Ein insgesamt sicheres Logon umfasst den Registrierungsprozess (Ein-/Auslernen von Nutzern), die (graphische) Logon-Schnittstelle und die netzwerkseitige Authentisierung und sollte verschiedene Sicherheitsaspekte berücksichtigen. Hierzu gehören bspw. Anzahl der Fehlversuche, Passwortstärke (password policy), Prüfung auf schwache Passwörter, Schutz des Logon-Graphical User Interface (GUI) sowie eine gesicherte Netzwerkauthentisierung.

Eine mögliche Implementierungshilfe für die Maßnahme findet sich in:

- [VGB S-175]: 2.3.2.2 Zugriffskontrolle

4.7.4.4 Rollentrennung (Getrennte Admin-Konten)

Für administrative Tätigkeiten sollten entsprechende Accounts (Konten) mit erweiterten Privilegien zur Verfügung stehen. Die Nutzung dieser sogenannten Adminaccounts beschränkt sich ausschließlich auf die einzelne, administrative Tätigkeit. Diese Admin-Tätigkeiten sind entsprechend zu dokumentieren. Für alle anderen, nicht administrativen Aufgaben und Tätigkeiten sollten auch Administratoren stets mit ihrem normalen Benutzeraccount arbeiten.

Eine mögliche Implementierungshilfe für die Maßnahme findet sich in:

- [VGB S-175]: 2.3.2.1 Authentisierung
- [ISO/IEC 27001]: A 9.1.1 Zugangssteuerungsrichtlinie

4.7.5 Verschlüsselung

4.7.5.1 Kryptografische Absicherung

Grundsätzlich sollte eine Verschlüsselungsstrategie für gespeicherte Daten (data in rest) und Daten, die sich in der Verarbeitung befinden (data in motion) definiert werden.
Dabei gilt es, ein dem Schutzbedarf angemessenes Verschlüsselungsverfahren zu wählen, um den Schutz der Daten vor unberechtigtem Zugriff zu gewährleisten.

Eine mögliche Implementierungshilfe für die Maßnahme findet sich in:

- [BSI TR-02102-1]: Kryptographische Verfahren: Empfehlungen und Schlüssellängen
- [ISO/IEC 27001]: A 8.3.1 Handhabung von Wechseldatenträgern

4.7.5.2 Cloud-Daten-Verschlüsselung (Cloud-Encryption)

Für die Cloud-Daten-Verschlüsselung sollte neben der verschlüsselten Speicherung von Daten in der Cloud insbesondere auch eine

Transportverschlüsselung für den Übertragungsweg wie bspw. HTTPS eingesetzt werden.

Die hierfür erforderlichen privaten Schlüssel sollten entsprechend gesichert verwahrt werden.

Eine mögliche Implementierungshilfe für die Maßnahme findet sich in:

- [ISO/IEC 27001]: A 9.4.2 sichere Anmeldeverfahren

4.7.5.3 Verschlüsselung der Kommunikationsverbindungen (z.B. Voice Encryption)

Es sollte eine Verschlüsselung von kritischen und unter den Aspekten von Informationssicherheit und Datenschutz relevanten Kommunikationsverbindungen durchgeführt werden, um bspw. das Abhören und Verfälschen von Inhalten auszuschließen.

Eine mögliche Implementierungshilfe für die Maßnahme findet sich in:

- [ISO/IEC 27001]: A 10.1.1 Richtlinie zum Gebrauch von kryptographischen Maßnahmen

4.7.5.4 E-Mail-Verschlüsselung

Es sollte die Option einer E-Mail-Verschlüsselung und -Signierung zum Einsatz kommen, damit bei Bedarf die Vertraulichkeit und Integrität des Emailinhalts gewahrt und die Authentizität des Absenders geprüft werden kann.

Eine mögliche Implementierungshilfe für die Maßnahme findet sich in:

- [ISO/IEC 27001]: A 10.1.1 Richtlinie zum Gebrauch von kryptographischen Maßnahmen

4.7.5.5 Verschlüsselung der Datenträger z. B. Festplattenverschlüsselung

Für Daten auf mobilen Datenträgern (CDs, USB-Sticks, externe Festplatten etc.) sollte eine beschränkte Nutzung nur durch befugte Personen sichergestellt sein. Dieses kann mit Hilfe von Datenträgerverschlüsselungen erfolgen (siehe hierzu auch 4.7.5.1) oder durch Verwahrung in einem entsprechend geschützten Sicherheitsbereich.

Eine mögliche Implementierungshilfe für die Maßnahme findet sich in:

- [ISO/IEC 27001]: A 8.3.1 Handhabung von Wechseldatenträgern

4.7.5.6 Aufrechterhaltung des aktuellen Informationsstands durch Bezug von Warnungen, CERT-Meldungen, Lagebild

Der Betreiber sollte sicherstellen, dass er jederzeit über einen aktuellen Informationsstand bezüglich der für die kDL VvFw relevanten

Informationssicherheitslage verfügt, unter anderem über die Cyber-Sicherheitswarnungen des BSI Lagezentrums oder im Rahmen der kooperativen Partnerschaft im UP KRITIS.

Eine mögliche Implementierungshilfe für die Maßnahme findet sich in:

- [ISO/IEC 27001]: A 6.1.3 Kontakt mit Behörden

4.8 Physische Sicherheit

Zum Schutz der für die Funktionsfähigkeit der kDL VvFw maßgeblichen IT-Systeme müssen physische Sicherheitsvorkehrungen vor Naturkatastrophen oder anderen umweltbedingten Beeinträchtigungen entsprechend einer Risikobewertung konzipiert und getroffen werden. Diese sind in Sicherheitskonzepten, die bauliche, organisatorische und technische Maßnahmen für die physische Sicherheit umfassen, festzulegen und im weiteren Verlauf regelmäßig zu überprüfen. Hierbei sind u. a. folgende Sicherheitsmaßnahmen näher zu betrachten:

- Schutz vor Feuer und Explosionen unter Berücksichtigung der jeweiligen Bauvorschriften,
- Schutz vor Überschwemmungen, insbesondere in unterirdischen Einrichtungen, z.B. durch selbstständige Entwässerungen,
- Ausstattung des Gebäudes der Leitwarte mit Blitzschutzeinrichtungen (Blitzableitern).

4.8.1 Zugangskontrolle

Weiterhin müssen die eingesetzten IT-Systeme angemessen vor Beschädigung oder Zerstörung durch Unfälle und vorsätzliche Angriffe geschützt werden. Folgende Maßnahmen sind hierbei u.a. zu betrachten:

- Das Betriebsgelände ist sichtbar und eindeutig durch physische Barrieren zu begrenzen, um unberechtigtes Eindringen auf das Betriebsgelände zu erschweren (Zäune, Mauern, einbruchshemmende Türen und Fenster etc.).
- Es ist zu gewährleisten, dass nur für den Zutritt berechtigte Personen auf das Betriebsgelände gelangen können.
- Besucher und bereichsfremde Personen sind in entsprechenden Örtlichkeiten (z.B. Pförtnerhaus, Empfangshalle etc.) in Empfang zu nehmen, an- und abzumelden und standortspezifisch einzuweisen.
- Zum Schutz vor nicht autorisiertem Zutritt/Zugang zu Betriebseinrichtungen und Betriebsmitteln sind Schließsysteme oder andere Zugangskontrollsysteme einzurichten (abschließbare Türen/Schränke/Safes inklusive Schlüsselverwaltung)
- Festlegung von Sicherheitszonen mit definiertem Sicherheitsumfang und -anforderungen in Abhängigkeit der Kritikalität der darin befindlichen Informationen und IT-Systeme.
- Pförtner oder Mitarbeiter der Haustechnik sollten regelmäßig überprüfen, ob Fenster und Türen nach Verlassen von Räumen verschlossen wurden.
- Zugangspunkte mit häufigem Publikumsverkehr (z.B. Anlieferungs- und Ladezonen) bilden ein besonders gefährdetes Einfallstor für nicht-autorisierten Zugang zu

Betriebsstätten und sind daher nach Möglichkeit von informationsverarbeitenden Einrichtungen zu isolieren sowie verstärkt zu kontrollieren.
- Festlegung und aktive Verwaltung von Zugangs- und Zutrittsrechten.
- Installation geeigneter Einbruchmeldeanlagen (Alarmanlagen) in Abhängigkeit der Risikoklassifikation.

4.8.2 Strom-/Notstromversorgung und Netzersatzanlagen

Zudem sind die für die Erbringung der kDL VvFw maßgeblichen IT-Systemen hinsichtlich möglicher Stromausfälle zu betrachten. Hierbei sollten u.a. folgende Aspekte eingehalten und berücksichtigt werden:

- Sie müssen entsprechend der geltenden gesetzlichen Vorschriften sowie den Spezifikationen des Herstellers eingerichtet sein und regelmäßig auf ordnungsgemäße Funktionalität überprüft werden
- Sie sind regelmäßig auf eine ausreichende Auslegung zu überprüfen (z. B. hinsichtlich der geschäftlichen Anforderungen und/oder Interaktion mit anderen Versorgungs-einrichtungen)
- Stromkreise sollten soweit möglich unterteilbar/segmentierbar sein und bei Bedarf mehrere Zuführungen über unterschiedliche Zuleitungswege besitzen
- Stromkabel sollten auf geeignete Weise vor äußerlichen Beeinträchtigungen oder Beschädigungen geschützt sein, z.B. durch eine unterirdische Verlegung und ggf. Abschirmung, um ein Übersprechen auf die Datenleitungen zu verhindern
- Netzwerk- und Systemkomponenten, die der Messung, Überwachung, Steuerung und Regelung der kDL VvFw dienen, sind dahingehend zu bewerten, ob diese durch eine unterbrechungsfreie Stromversorgung (USV) und Netzersatzanlage abgesichert sein sollten

4.9 Weitere Maßnahmen

4.9.1 Personelle und organisatorische Sicherheit

Zur Sicherstellung der kDL VvFw sind neben den Aspekten der technischen Informationssicherheit auch Maßnahmen zur Gewährleistung der personellen und organisatorischen Sicherheit durch den Betreiber umzusetzen.

Hierzu gehören bspw.:

- regelmäßige Informationssicherheitsschulungen und Sensibilisierungsmaßnahmen für alle relevanten internen und externen Mitarbeiter
- die Sicherstellung der für einen den Anforderungen für die Erbringung der kDL entsprechenden Betriebs notwendigen qualifizierten, personellen Ressourcen,
- Sicherheits- bzw. Hintergrundüberprüfungen des Personals gemäß den gesetzlichen Vorgaben

- die Schaffung von Verständnis (Awareness) für Informationssicherheit auf allen Mitarbeiterebenen durch das aktive Bekenntnis der Unternehmensleitung zur Informationssicherheit, die von allen Beschäftigten und Auftragnehmern die Einhaltung und Umsetzung der etablierten Informationssicherheitsvorgaben und -verfahren verlangt. Die Vorgaben und Verfahren sind dokumentiert, unternehmensintern veröffentlicht und Ansprechpartner sind in der Organisation als fachliche Kontaktstellen eingerichtet worden
- der Aufbau einer bedarfsgerechten Informationssicherheitsorganisation,
- die Festlegung von definierten Verantwortlichkeiten (Rollen), Rechten, Befugnissen und Berechtigungen sowie die Sicherstellung einer entsprechenden Vertretungsregelung unter Berücksichtigung eines Vieraugenprinzips und einer Funktionstrennung, wo dieses erforderlich ist
- die Etablierung eines geeigneten Identity & Access Managementsystems (IAM)
- ein geeignetes Verfahren zur Dokumentation von Ausnahmeregelungen
- ein adäquates Vorfallmanagementsystem (siehe auch Abschnitt 4.3)

4.9.2 Überprüfung im laufenden Betrieb

Die Wirksamkeit der getroffenen Maßnahmen zum Schutz der, für die Funktionsfähigkeit der kDL VvFw maßgeblichen informationstechnischen Systeme, Komponenten und Prozesse, muss regelmäßig in geeigneter Weise überprüft werden, bspw. unter Anwendung von Penetrationstests nach ISO/IEC 27002 Abschnitt 18.2. Diese Überprüfungen sollten z. B. im Rahmen von Audits oder bei regulären Teilbereichsprüfungen stattfinden. Hierzu gehören bspw. anlassbezogene Prüfungen aufgrund von Änderungen der Bedrohungs-/Gefährdungslage, nach erfolgreichen oder potenziell erfolgreichen Angriffen und nach Änderungen an IT- oder Kommunikationssystemen.

4.9.3 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 ist eine Informationsversorgung und Unterstützung zweckmäßig. Hierzu gehören bspw. die Änderung der Bedrohungslage, Bedrohungs- bzw. Schwachstelleninformationen. Zudem sollten geeignete Verfahrensweisen und Schnittstellen für den Erhalt externer sicherheitsrelevanter Informationen (wie bspw. Cyber-Sicherheitswarnmeldungen des BSI-Lagezentrums) sowie zum Abruf von Unterstützungsleistungen eingerichtet und gepflegt werden.

4.9.4 Lieferanten, Dienstleister und Dritte

Es sind Verfahrensweisen zu etablieren, um Lieferanten, Dienstleister und Dritte entsprechend der geltenden Informationssicherheitsanforderungen auszuwählen. Diese sind auf die Einhaltung der Informationssicherheitsanforderungen zu verpflichten. Die Umsetzung der Vorgaben ist zu steuern und zu überwachen. Anzuwenden sind die Informationssicherheitsanforderungen bspw. auf Produkte, die von Lieferanten bezogen werden, auf Dienstleister, die in den Betrieb der kDL VvFw oder die Wartung von hierfür relevanten informationstechnischen Systemen oder Komponenten eingebunden werden und auf Geschäftsprozesse und Leistungen, die an Externe ausgelagert worden sind.

Für geeignete Maßnahmen zum Umgang mit Lieferanten und Dienstleistern sind die Best-Practice Empfehlungen des BSI bzw. UP KRITIS für Anforderungen an Lieferanten zur Gewährleistung der Informationssicherheit in Kritischen Infrastrukturen zu berücksichtigen[1].

Eine weitere Hilfestellung bietet das BDEW/OE Whitepaper „Anforderungen an sichere Steuerungs- und Telekommunikationssysteme“.

5 Nachweisbarkeit der Umsetzung

Auf Grund sich ggf. verändernder gesetzlicher Grundlagen während des Gültigkeitszeitraumes für die Eignung dieses B3S VvFw kann zur Erfüllung der Anforderungen gemäß § 8a Absatz 1 in Verbindung mit Absatz 3 BSIG an dieser Stelle nur der Hinweis auf die zum Zeitpunkt der Erstellung dieses B3S VvFw geltende Gesetzeslage gegeben werden. Dieser befindet sich in der Anlage 1 und ist nicht Bestandteil der Eignungsprüfung durch das BSI und ist bzgl. der jeweils gültigen Gesetzeslage zu überprüfen.

[1] https://www.kritis.bund.de/SharedDocs/Downloads/Kritis/DE/Anforderungen_an_Lieferanten.html

Literaturverzeichnis

AGFW FW 1000	Anforderungen an die Qualifikation und die Organisation technischer Bereiche von Kraftwerksbetreibern sowie Wärmeversorgungsunternehmen
AVBFernwärmeV	Verordnung über Allgemeine Bedingungen für die Versorgung mit Fernwärme
BDEW/OE Whitepaper (2018)	BDEW, Oesterreichs Energie: Whitepaper Anforderungen an sichere Steuerungs- und Telekommunikationssysteme Vollständig überarbeitete Version 2.0 05/2018 BDEW Bundesverband der Energie- und Wasserwirtschaft e. V., Oesterreichs E-Wirtschaft Wien/Berlin, 8. Mai 2018
BSI TR-02102-1	„Kryptographische Verfahren: Empfehlungen und Schlüssellängen“; Version: 2020-01
DIN EN ISO/IEC 17021	Konformitätsbewertung - Anforderungen an Stellen, die Managementsysteme auditieren und zertifizieren
[ISO/IEC 27001]: ISO/IEC 27001:2013 (inkl. Cor.1:2014 & Cor. 2:2015) oder DIN EN ISO/IEC 27001:2017	Original-Titel (Englisch) Information technology - Security techniques - Information security management systems - Requirements Überarbeitete Übersetzung (Deutsch) IT-Sicherheitsverfahren – Informationssicherheits-Managementsysteme – Anforderungen
[ISO/IEC 27002]: ISO/IEC 27002:2013 (inkl. Cor.1:2014 & Cor. 2:2015) oder DIN ISO/IEC 27002:2013	Original-Titel (Englisch) Information technology - Security techniques - Code of practice for information security controls Übersetzung (Deutsch) Informationstechnik - Sicherheitsverfahren - Leitfaden für Informationssicherheitsmaßnahmen
ISO/IEC 27005:2018	Original-Titel Information technology - Security techniques - Information security risk management Übersetzung (Deutsch) Informationstechnik - IT-Sicherheitsverfahren - Informationssicherheits-Risikomanagement
[ISO/IEC 27006]: ISO/IEC 27006:2015-10 oder ISO/IEC 27006:2015-10	Original-Titel Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems Übersetzung (Deutsch)

	Informationstechnik - IT-Sicherheitsverfahren - Anforderungen an Institutionen, die Audits und Zertifizierungen von Informationssicherheits-Managementsystemen anbieten
ISO 31000:2018	Original-Titel Risk Management-Guidelines
DIN ISO 31000: 2018	Übersetzung (Deutsch) Risikomanagement-Leitlinien
Orientierungshilfe zu Nachweisen gemäß § 8a (3) BSIG	Bundesamt für Sicherheit in der Informationstechnik Version 1.0 vom 15.05.2019
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
VGB-S-175-00-2014-04-DE	Technischer Standard des VGB PowerTech Titel (Deutsch) IT-Sicherheit für Erzeugungsanlagen