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: 03. Mai 2018

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
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
PDH	Plesiochrone Digitale Hierarchie (ist eine international standardisierte Technik zum Multiplexen digitaler Datenströme, die über Weitverkehrsstrecken übertragen werden. Die Datenströme müssen annähernd synchron sein)
RL	Rücklauf
RTU	Remote Terminal Unit (Fernbedienungsterminal)
SCADA	Supervisory Control and Data Acquisition (Überwachen und Steuern technischer Prozesse mittels eines Computer-Systems)
SDH	Synchrone Digitale Hierarchie (ist eine der Multiplextechniken im Bereich der Telekommunikation, die das Zusammenfassen von niederratigen Datenströmen zu einem hochratigen Datenstrom erlaubt. Das gesamte Netz ist dabei synchron.)
SPS	Speicherprogrammierbare Steuerung
SDH	Synchrone Digitale Hierarchie
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
z. B.	Zum Beispiel

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 27001:2013 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 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. Der hier betrachtete Teil der kritischen Dienstleistung (kDL) Versorgung mit Fernwärme in diesem Sinne ist die Verteilung von Fernwärme (VvFw).

Die leitungsgebundene Verteilung von Fernwärme steht im direkten Wettbewerb mit 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.

1.2 Geltungsbereich

Als Fernwärmeverteilung bezeichnet man die Versorgung mit Wärme über Liegenschaftsgrenzen hinweg. Fernwärme wird in Form von heißem Wasser verteilt, in einzelnen wenigen Fällen bestehen noch Fernwärmesysteme, die die Wärme auf Basis von Dampf verteilen. 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). Vermaschte Verbundnetze sind hinsichtlich der Versorgungssicherheit besonders sicher; fällt die Wärmelieferung einer Erzeugungsanlage aus, kann dies durch das Verbundnetz sofort ausgeglichen werden. Ebenso kann durch Schaltmaßnahmen im Netz 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.

Für die Sicherstellung der Versorgung werden Fernwärmesysteme in der Regel nach dem Prinzip der n-1-Sicherheit ausgelegt. D.h. bei Ausfall der größten einzelnen Wärmeerzeugungsanlage wird noch immer die maximal vorzuhaltende Leistung erreicht. Die Auslegung und Dimensionierung von Fernwärmesystemen erfolgt auf Grundlage einer minimal anzunehmenden Außentemperatur als Tagesmittelwert nach DIN 4710 / DIN EN 12831. Danach sind Fernwärmesysteme in Deutschland für unterschiedliche Auslegungstemperaturen konzipiert, z.B. -10°C für Bonn, -12°C für Hamburg und -14°C für Berlin. Diese Auslegungstemperaturen werden im Durchschnitt nur zehnmal in 20 Jahren als Tagesmittelwert der Außentemperatur erreicht. Dadurch werden die maximal vorzuhaltenden Leistungen von Fernwärmesystemen in der Praxis nicht abgefordert.

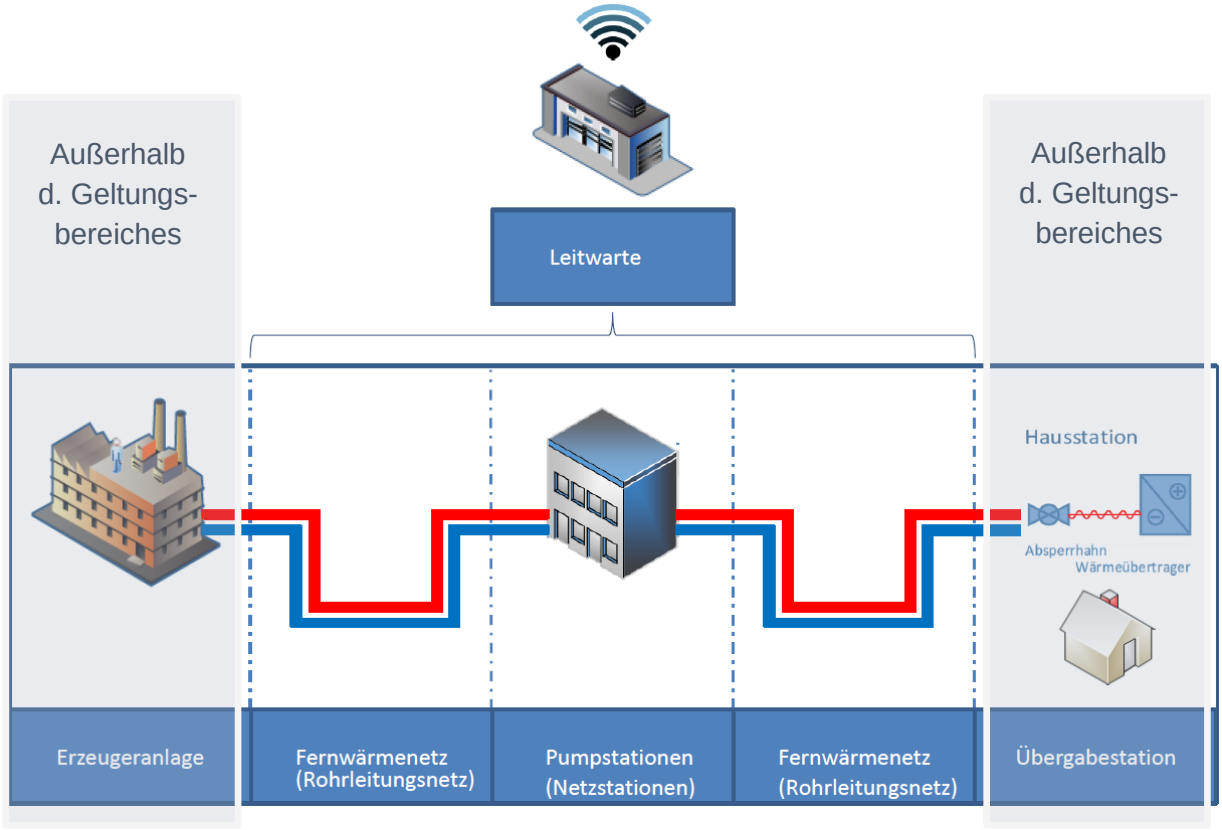

Abb. 1: Darstellung Fernwärmenetz

Fernwärmenetze bestehen aus fünf wesentlichen Baugruppen[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

[1] Quellen:
- https://www.agfw.de/kundenanlagen/hausuebergabestation/dampf-uebergabestation/

Raumheizung und einen als Konstantwärmeleiter für die hausinterne Warmwasserbereitung)

2. Den Pumpstationen zur Druckerhöhung. Die Druckerhöhung dient zur Überwindung der Druckverluste im Fernwärmenetz und damit zum Transport der Fernheizwassermengen.
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 optimalen Fahrweise des Fernwärmenetzes sowie der einspeisenden Erzeugungsanlagen.
4. Die zentrale Leittechnik unterstützt das Leitwarten-Personal bei ihren Aufgaben. Sie ist generell eine Schnittstelle zur Überwachung des Fernwärmenetzes. Mit ihrer Hilfe werden Fernwärmenetzzustände, Lastprognosen, Fahrpläne abgebildet. Über die zentrale Leittechnik werden z.B. Drehzahländerungen an Pumpen eingestellt. Die Signale werden mittels Fernwirktechnik z.B. an die Speicherprogrammierbare Steuerung (SPS) der Pumpen übertragen. Die SPS der Pumpen setzt diese dann in die Drehzahl um. Auch Störmeldungen aus dem Fernwärmenetz werden dargestellt und können so effizient abgearbeitet werden.
5. Die Übergabestation (technische Einrichtung) ist das Bindeglied zwischen Rohrleitungsnetz und Hauszentrale des Kunden. Sie befindet sich in der Regel im Verantwortungsbereich und Gebäude des Kunden. Sie dient dazu, die Wärme bestimmungsgemäß, z. B. hinsichtlich Druck, Temperatur und Volumenstrom, an die Hauszentrale zu übergeben.

Die Anlagen des Kunden stehen außerhalb des Geltungsbereichs des B3S VvFw.

Auf der Kundenseite befinden sich :

- die Übergabestation,
- die Hausanlage, bestehend aus dem Rohrleitungssystem ab Hauszentrale, den Heizflächen sowie den zugehörigen Absperr-, Regel- und Steuereinrichtungen.

Weiterhin außerhalb des Geltungsbereichs des B3S VvFw stehen die Erzeugungsanlagen für die Bereitstellung der Wärme (z.B. Heizkraftwerke und Heizwerke).

Das Rohrleitungsnetz fällt nur dann in den Anwendungsbereich des B3S VvFw, wenn dort IT-technische Einrichtungen zum Einsatz kommen, die Auswirkungen auf den Betrieb der

kritischen Infrastruktur haben könnten. Zur Zeit sind am Markt jedoch keine derartigen Einrichtungen bekannt.

Die Verteilung von Fernwärme erfolgt durch den Einsatz von Pumpen in den Pumpstationen. Pumpen können entweder analog oder digital gesteuert betrieben werden (siehe Abb. 2) Bei einer digitalen Steuerung sorgen IT-Systeme für die Funktionsfähigkeit. Bei Verwendung einer analogen Steuerung können die Pumpen komplett manuell vor Ort bedient werden. Zur Umsetzung einer betriebswirtschaftlich optimierten Steuerung kann vor Ort bei den Pumpen eine digitale Steuerung (z.B. SPS speicherprogrammierbare Steuerung) auf die analoge Steuerung aufgesetzt werden. Diese Steuerungen können wiederum mit einer zentralen Leitwarte über eine Fernwirktechnik verbunden sein. Grundsätzlich können die Pumpen auch durch manuelle Schalthandlungen vor Ort in eine manuelle Betriebsweise umgeschaltet werden und mittels der vor Ort vorhandenen Steuerungstechnik (z.B. SPS) bzw. mittels analoger Manometer und Thermometer von Hand betrieben werden.

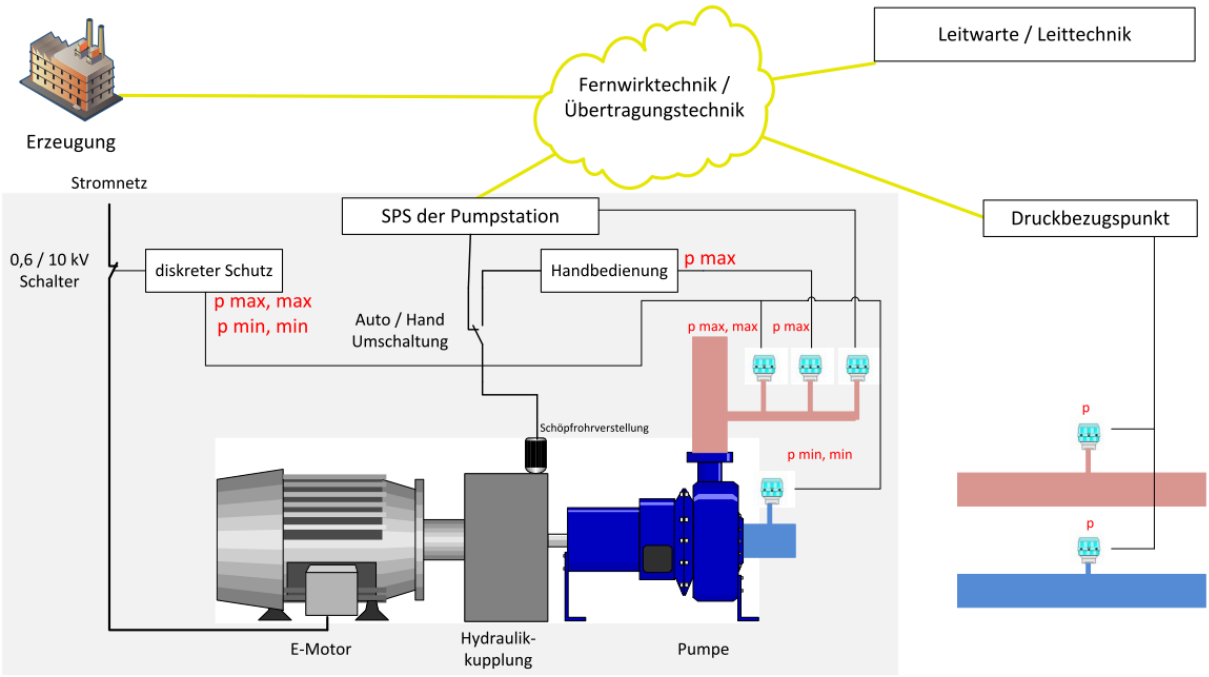

Abb. 2.: Fernwärmeverteilung (mit optionaler Anbindung an eine Leitwarte mittels Leittechnik)

1.3 Geltungsbereich für extern erbrachte Leistungen

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

1.4 Gesetzlicher Rahmen

Die AVBFernwärmeV ist die Vertragsgrundlage für die Fernwärmelieferung an Endkunden.

2 Schutz der kritischen Dienstleistung (KRITIS-Schutzziele)

Das Schutzziel der kDL Fernwärmeversorgung gem. 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). In allgemeinen Großkrisen und IT-Krisenlagen 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 VvFw notwendig ist.

Zur Erfüllung der kritischen Dienstleistung muss die Verfügbarkeit und Funktionsfähigkeit der erforderlichen Infrastrukturen zum Transport des heißen Wassers oder des Dampfes zur Fernwärmeversorgung gewährleistet werden.

Hierzu wird durch die Erzeugungsanlagen eine Vorlauf-Temperatur von zum Beispiel 90 °C bereitgestellt. Die zu erbringende Wärmeleistung (Wärmeenergiemenge pro Zeiteinheit) ist mit den Kunden vertraglich vereinbart und wird in Volumen (Liter Wasser) zur Übergabestation geliefert. Die gewünschte Temperatur im Heizungssystem wird durch den Kunden eigenständig reguliert.

Je nach Betriebsstrategie werden die Pumpstationen mittels Übertragungstechniken von der Leitwarte angesteuert und überwacht. Die Übertragung kann durch das Internet aber auch durch, von der Öffentlichkeit vollkommen getrennten, Übertagungstechnik erfolgen. Diese Fernwirktechnik sind z.B. SDH oder PDH Netze.

Maßnahmen zur Erfüllung des KRITIS-Schutzziels beziehen sich ausschließlich auf informationstechnische Systeme, Komponenten oder die Prozesse, die für die Funktionsfähigkeit der kritischen Infrastrukturen 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. Dies umfasst die Auswahl angemessener organisatorischer und technischer Vorkehrungen hinsichtlich:

- der Sicherstellung der Verfügbarkeit der zu schützenden Systeme und Daten,

- der Sicherstellung der Integrität der verarbeiteten Informationen und Systeme,
- der Sicherstellung der Authentizität der beteiligten Systeme, Komponenten, Prozesse und Personen in der Informationsverarbeitung sowie
- der Gewährleistung der Vertraulichkeit der mit den betrachteten Systemen verarbeiteten Informationen.

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 die Fernwirktechnik, sind folgende anlagenspezifische Schutzziele zu berücksichtigen:

1) Verfügbarkeit: Bedeutet, dass bei einer digitalen Steuerung der Fernwärmepumpen die hierfür verwendeten IT-Systeme und Fernwirktechniken verfügbar, d.h. funktionsfähig, sind.
2) Integrität: Bedeutet, dass digitale Steuerungsimpulse, die vom IT-System ausgehen, unverfälscht in der Leitwarte ankommen und umgesetzt werden, sowie digitale Impulse der Leitwarte unverfälscht beim IT-System ankommen und umgesetzt werden.
3) Authentizität: Bezeichnet die Eigenschaften der Echtheit, Überprüfbarkeit und Vertrauenswürdigkeit des Absenders von übermittelten Daten. Diese Überprüfung wird als Authentifikation des Datenursprungs 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 VvFw jedoch nur in Ausnahmefällen von Relevanz.

2.3 Maßgeblichkeit der IT

Die IT ist für die Funktionsfähigkeit der FW-Verteilung maßgeblich, wenn

- diese für den Regelbetrieb der Verteilung der Fernwärme an Haushalte benötigt wird und
- diese angeschlossenen Haushalte im Falle einer Störung oder eines Ausfalls der eingesetzten IT über einen Zeitraum von mindestens 24 h keine Wärmelieferung erhalten.

Sollten die o.g. Voraussetzungen zutreffen, kann davon ausgegangen werden, dass die kritische Dienstleistung nicht mehr erbracht werden kann.

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

Die Nicht-Maßgeblichkeit der IT muss durch den Betreiber der kritischen Infrastruktur nachgewiesen werden. Der Nachweis umfasst insbesondere die Beschreibung der organisatorischen und technischen Maßnahmen, welche ermöglichen, dass die VvFw auch ohne IT manuell aufrecht erhalten werden kann. Beispiele hierzu finden sich in Kapitel 3.3.3.

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

3 Risikomanagement

3.1 Dokumentation des Anwendungsbereiches

Vor Beginn der Risikoanalyse müssen alle informationstechnischen Systeme, Komponenten oder Prozesse, die maßgeblich für die Funktionsfähigkeit der VvFw sind, erfasst, 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 -steuerung. Sie ermittelt die Auswirkungen, die eine Verletzung der Schutzziele der Informationssicherheit auf die Erbringung der kritischen Dienstleistung hätte.

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), über die die Informationen übertragen werden.

Im folgenden Schritt werden für alle Informationswerte die möglichen Schadensauswirkungen auf die VvFw bei Verletzung der relevanten Schutzziele (Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit) bewertet. Die entsprechend zugehörige Infrastruktur erbt die Bewertung der Informationen. Für die Einordnung der Auswirkungen eignen sich Schadenskategorien/ -stufen, z.B. von „1-gering“ bis „5-katastrophal“. Die genaue Festlegung der Schadenskategorien und deren Bedeutung für die VvFw ist vom Anwender im Vorfeld der Business Impact Analyse zu definieren, wobei ein Ausfall, der mehr als 125.000 Haushalte betrifft, in der höchsten Kategorie aufzuführen ist.

3.3 Branchenspezifische Gefährdungslage

Eine Gefährdung im Sinne des B3S 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 VvFw führen kann (Schadensauswirkung gem. BIA siehe oben). Eine Gefährdung realisiert sich, indem sie eine Schwachstelle in einer Infrastruktur ausnutzt.

3.3.1 Allgefahrenansatz

Im Rahmen eines Allgefahrenansatzes müssen regelmäßig alle relevanten Gefährdungen, die auf die im Anwendungsbereich befindlichen Informationswerte und deren Infrastruktur wirken, identifiziert werden. Aus diesen Gefährdungen werden Risiken für die VvFw 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 VvFw sind:

Nr.	Gefährdung	Relevanz für die VvFw (Hinweise zum Gefährdungspotential)
1	Physikalische Beeinträchtigung durch Naturgefahren - Physische Beeinträchtigung (Ausfall, Zerstörung) der Systeme durch verschiedene Umweltbedingungen - Nichtverfügbarkeit von Betriebsstätten durch verschiedene Umweltbedingungen	- Blitzeinschläge in oberirdischen Gebäuden (z.B. Leitwarte, oberirdische Pumpstationen) - Hochwasser insb. in unterirdischen Pumpstationen (z.B. durch Starkregen oder Grundwasseranstieg) - Wärme und/oder hohe Luftfeuchtigkeit, falls keine Klimatisierung vorhanden - Gefährdung durch Feuer
2	Unterbrechung der Stromversorgung	- Kann zum Ausfall der ITK-Systeme zur Steuerung und/oder Überwachung der Pumpen und Leitsysteme führen ➢ Ausfall der Technik auf der Leitwarte oder der Fernwirktechnik, somit keine Fernsteuerung/Überwachung mehr möglich ➢ Keine Bedienung und Steuerung der Pumpen und Anlagen im Netz von der Leitwarte mehr möglich (Betriebsstörung)

3	Zerstörung von Systemen - Durch physikalische Gefährdungen (siehe Nr.1) - Durch Angriffe / mutwillige Zerstörung - Durch versehentliche Zerstörung (z.B. Unachtsamkeit eines Mitarbeiters)	- Zerstörung der ITK-Systeme zur Steuerung und/oder Überwachung der Pumpen und Leitsysteme ➢ Zerstörung der Technik auf der Leitwarte oder der Fernwirktechnik, somit keine Fernsteuerung/Überwachung mehr möglich ➢ Keine Bedienung und Steuerung der Pumpen und Anlagen im Netz von der Leitwarte aus mehr möglich (Betriebsstörung)
4	Ausfall von Systemen/Services - Technisches Versagen von IT-Systemen, Anwendungen oder Netzen	- Ausfall der ITK-Systeme zur Steuerung und/oder Überwachung der Pumpen, Leitsysteme ➢ Ausfall der Technik auf der Leitwarte oder der Fernwirktechnik, somit keine Fernsteuerung/Überwachung mehr möglich ➢ Keine Bedienung und Steuerung der Pumpen und Anlagen im Netz von der Leitwarte aus mehr möglich (Betriebsstörung)
5	Ausspähen von / Unberechtigter Zugriff auf Daten - Daten werden ausgespäht bzw. es wird auf Daten zugegriffen, ohne dass man entsprechende Rechte besitzt	- Ausspähen von / Unberechtigter Zugriff auf Nutzerzugänge ➢ nicht autorisierter Zugriff und Nutzung von Daten oder Software kann zu Missbrauch & Veränderung führen - Ausspähen von Netzwerkinformationen (IP-Adressen), Netzstrukturpläne (Topologie des ITK-Systems) kann zum Durchführen gezielter Angriffe führen - Dieser Punkt ist nur relevant, wenn die Fernwirktechnik öffentlich zugänglich ist
6	Missbrauch & Veränderung von Daten	- Fehlerhafte / missbräuchliche Steuerung des Fernwärmenetzes kann zu Unterversorgungen im Netz führen, wenn z.B. Pumpen runter gefahren werden

		- Meldungen / Unregelmäßigkeiten werden ggf. nicht sofort erkannt und somit erst später durch das Betriebspersonal korrigiert / behandelt - Veränderung von Protokolldaten kann zu falscher Reaktion auf Unregelmäßigkeiten oder Störungen führen
7	Verlust und Offenlegung von Daten	- Verlust und Offenlegung des Datenmodells in der zentralen Leittechnik zur Steuerung des Fernwärmenetzes (Rohrleitungen, Pumpen), wenn diese für die VvFw notwendig ist
8	Missbrauch & Fälschung von Berechtigungen	- Unbefugter Zugriff auf Nutzerzugänge ➢ nicht autorisierter Zugriff und Nutzung von Daten oder Software kann zu Missbrauch & Veränderung führen - Eigentlich berechtigte Person kann nicht mehr auf Daten und Systeme zugreifen und somit ihrer Arbeit nicht nachgehen
9	Abstreiten von Aktionen (menschliche Fehlhandlungen, menschliches Versagen)	- Nachvollziehen von Fehlern nicht möglich
10	Manipulation an Software	- Schädigung, Zerstörung oder Ausfall der ITK-Systeme zur Steuerung und/oder Überwachung der Pumpen und Leitsysteme - Missbrauch, Veränderung oder Verlust von Daten
11	Fehlerhafte Software, Firmware & Hardware - Technische Schwachstellen in Software, Firmware und Hardware	- Schädigung, Zerstörung oder Ausfall der ITK-Systeme zur Steuerung und/oder Überwachung der Pumpen und Leitsysteme - Ausnutzbare Schwachstellen im Leitsystem, in der Leit- und Übertragungstechnik oder in unterstützenden Systemen
12	Fehlerhafte Administration von Systemen (menschliche Fehlhandlungen, menschliches Versagen)	- Schädigung, Zerstörung oder Ausfall der ITK-Systeme zur Steuerung und/oder Überwachung der Pumpen und Leitsysteme - Verlust von Daten

13	Fehlerhafte Bedienung von Systemen (menschliche Fehlhandlungen, menschliches Versagen)	- Schädigung, Zerstörung oder Ausfall der ITK-Systeme zur Steuerung und/oder Überwachung der Pumpen und Leitsysteme - Verlust von Daten
14	Nichtautorisierte Nutzung von Daten oder Software	- Schädigung, Zerstörung oder Ausfall der ITK-Systeme zur Steuerung und/oder Überwachung der Pumpen und Leitsysteme - Missbrauch, Veränderung oder Verlust von Daten
15	Verwendung von Daten oder Software aus nicht vertrauenswürdigen Quellen	- Ausnutzbare Schwachstellen im Leitsystem, in der Leit- und Übertragungstechnik oder in unterstützenden Systemen - Schadcode wird in Systeme eingebracht
16	Diebstahl von Medien oder Dokumenten	- Verlust von Back-Ups, Systemdokumentation, Systemkonfiguration
17	Zerstörung oder Ausfall von Ausrüstung oder Medien	- Zerstörung oder Ausfall von Ausrüstung in den Anlagen/Pumpstationen (Speicherprogrammierbare Steuerung, Schalteinrichtungen, Kabel) - Zerstörung oder Ausfall von Technik in der Leitwarte
18	Nichtautorisierte Nutzung von Ausrüstung	- Nutzung von Parametriergeräten zur Manipulation oder nichtautorisierter Steuerung der Pumpen - Missbrauch, Veränderung oder Verlust von Daten
19	Diebstahl von Ausrüstung	- Diebstahl von Parametriergeräten, was zu Verzögerungen im Betriebsablauf oder zu nichtautorisierter Nutzung führen kann
20	Schadcode wird in Systeme eingebracht	- Ausnutzung von Schwachstellen im zentralen Leitsystem, in der Leit- und Übertragungstechnik oder in unterstützenden Systemen - Schädigung, Zerstörung oder Ausfall der ITK-Systeme zur Steuerung und/oder Überwachung der Pumpen und Leitsysteme

		- Missbrauch, Veränderung oder Verlust von Daten
21	Verletzung der Instandhaltbarkeit von Informationssystemen - Informationssysteme können nicht mehr instandgehalten werden	- Veraltete Technik oder die Nicht-Beseitigung von Schwachstellen kann zur Schädigung, Zerstörung oder Ausfall der ITK-Systeme zur Steuerung und/oder Überwachung der Pumpen und Leitsysteme führen
22	Nichtverfügbarkeit von Personal - Es ist nicht genügend qualifiziertes Personal verfügbar	- Betrieb der ITK-Systeme zur Steuerung und/oder Überwachung der Pumpen und Leitsysteme nicht möglich - Reaktion auf Probleme / Störungen (in kritischen Betriebszuständen) nicht möglich
23	Bestechung oder Betrug	- Absichtliche fehlerhafte Administration oder Bedienung von Systemen
24	Nichteinhaltung von Vorgaben	- Schädigung, Zerstörung oder Ausfall der ITK-Systeme zur Steuerung und/oder Überwachung der Pumpen und Leitsysteme durch fehlerhafte Bedienung - Schadcode wird in Systeme eingebracht (z.B. durch Verwendung von Daten oder Software aus nichtautorisierten Quellen)
25	Nichtverfügbarkeit von Betriebsstätten	- Nichtverfügbarkeit von Leitwarte, Pumpstationen und Fernwirktechnik (sofern vorhanden)

3.3.3 Wirkungen von Gefährdungen oder Vorfällen ohne IT-Bezug auf die VvFw und deren Gegenmaßnahmen

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

In der Regel erlaubt die Speicherwirkung der Gebäude bzw. die Trägheit des gesamten Systems Total-Ausfallzeiten der Fernwärmeversorgung zwischen 3-5 Stunden ohne Komfortverlust in den Wohnungen. Nach 24 Stunden wird sich eine spürbare Raumtemperaturabsenkung einstellen.

Störungen und deren Auswirkungen auf die VvFw:

- Versorgungsausfälle oder -einschränkungen durch Störungen bei der Fernwärmeverteilung und Maßnahmen zur Absicherung:
    - Durch zu niedrige Umwälzmenge oder zu niedrige Vorlauf-Temperaturen können Teileinschränkungen der Versorgung eintreten. Zu niedrige Vorlauftemperaturen lassen sich durch höhere Umwälzmengen kompensieren und umgekehrt. Komfortverluste treten in der Regel erst nach ca. 10 Stunden auf, wenn die VL-Temperatur um 25% unterschritten wurde.
    - Bei zu geringer Wärme im Rohrleitungssystem wird der Erzeuger gebeten, mehr Wärme zu liefern. Einschränkungen oder Ausfälle bei der Wärmeeinspeisung betreffen die Wärmerzeugungsanlagen und sind durch das Fernwärmenetz nicht beeinflussbar.
    - Bei Störungen an einer Rohrleitung (z.B. durch einen Baggerschaden) ist im Normalfall eine Trennung von einzelnen Versorgungsteilen möglich, sodass die Versorgung nur teilweise eingeschränkt und die Funktionsfähigkeit des restlichen Fernwärmenetzes weiterhin sichergestellt ist. Die Trennungen in dem Fernwärme-Verbund-Netz erfolgen nach heutigem Stand der Technik ohne Leittechnik durch mechanische Schalthandlungen im Netz.
- Versorgungsausfälle oder -einschränkungen durch Störungen an Pumpen/ Pumpstationen und Maßnahmen zur deren Absicherung
    - Allgemein ist bei einer Störung oder Ausfall einzelner Pumpen ein „Bypassen“ möglich, d.h. auch bei Störungen wird die Versorgungsleistung aufrecht erhalten.
    - Manipulationen oder (mutwillige) Beschädigungen von Pumpen: Pumpstationen sind in der Regel unterirdische Gebäude, die über Zugangs- und Brandschutzsicherungen verfügen, so dass nur das dafür autorisierte Personal Zugang erhält.
    - Gefahr durch Überdruck: Zum Schutz gegen Überdruck sind in den Pumpstationen diskrete (separate) Sicherungen installiert (z.T. rein mechanisch, z.T. thermomechanisch), die im Gefahrenfall ohne IT oder Leittechnik auslösen.
    - Personalengpässe bei manuellem Betrieb z.B. im Störfall: Im Falle einer Umschaltung auf manuellen Betrieb wird der Druck im Vorlauf erhöht, sodass die Verteilung der Fernwärme weiter funktioniert, ohne dass Personal konstant vor Ort in den Pumpstationen anwesend sein muss. Eine regelmäßige Prüfung der Pumpstationen im Störungsfall - z. B. alle 4 Stunden - wird als ausreichend erachtet, um den höheren konstanten Druck zu prüfen und die Verteilung der Fernwärme zu sichern. Grundsätzlich ist sichergestellt, dass Techniker innerhalb dieses Zeitraumes zur Behebung von Störungen die betroffenen Pumpstationen aufsuchen können, so dass bei den Kunden auch bei

Umstellung auf kompletten Handbetrieb des gesamten Verteilnetzes kein Komfortverlust bezüglich der Raumtemperatur spürbar wäre.

Grundsätzlich ist durch den Betreiber der kritischen Infrastruktur sicherzustellen, dass im Falle von Störungen wirksame Entstörungsprozesse im Unternehmen etabliert sind.

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 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 Risikoanalyse

3.4.1 Feststellung und Bewertung von Risiken

Die unter Punkt 3.3.2 festgestellten Gefährdungen können wirksam werden, indem sie Schwachstellen in der Infrastruktur ausnutzen. Für die Abschätzung von Risiken muss die Eintrittswahrscheinlichkeit dieser Gefährdungen bestimmt werden. Eine anschließende Kombination der Eintrittswahrscheinlichkeit mit den, in der BIA ermittelten potenziellen Schadensauswirkungen, ergibt für jede Gefährdung ein Risiko, das 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 VvFw 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 nach Maßgabe des B3S im Vorfeld durch das Unternehmen festzulegen und zu begründen.

3.4.2 Techniken und Methoden zur Risikoanalyse & -Darstellung

Für eine aussagekräftige Risikobewertung sind bewährte Techniken anzuwenden. Folgende Bewertungsmethoden können z.B. benutzt werden:

- Checklisten
- Risikomatrix
- Szenario-Analysen
- Maßnahmen-Analyse

3.4.3 Bestimmung der Risikotoleranz

Die Risikotoleranz beschreibt das Maß der Bereitschaft, individuelle Risiken einzugehen. Sie bemisst sich an der Verfügbarkeit der VvFw, somit gilt prinzipiell ein hoher Schutzbedarf. Im Rahmen der Risikobewertung muss im Vorfeld definiert werden, wann ein Risiko auf einem annehmbaren Niveau liegt und ab wann weitere ursachen- oder wirkungsbezogene Maßnahmen notwendig sind. Einzelfallentscheidungen sind zu dokumentieren und zu überwachen.

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: Unterlassen von Aktivitäten, durch die ein Risiko entsteht
2. Risikoverminderung: Durch geeignete Schutzmaßnahmen wird die Eintrittswahrscheinlichkeit einer Bedrohung vermindert.
3. Risikobegrenzung: Durch geeignete Maßnahmen wird bei Eintreten eines Risikos der Schaden begrenzt.

Eine eigenständige dauerhafte Risikoakzeptanz relevanter Risiken für die VvFw ist im Sinne des BSIG keine zulässige Option. Auch eine Risikoüberwälzung, d.h. die teilweise oder vollständig Übertragung eines Risikos an Dritte ist nicht zulässig.

4.1 Angemessenheit und Eignung von Maßnahmen durch Einsatz branchenspezifischer Technik

Die im Rahmen der Risikobewältigung abgeleiteten Maßnahmen müssen angemessene organisatorische und technische Vorkehrungen zur Vermeidung, Verminderung oder Begrenzung der Risiken beinhalten. Diese gelten gemäß § 8a Abs. 1 Satz 3 BSIG dann als angemessen, wenn sie dem Stand der Technik entsprechen und wenn der zur Umsetzung erforderliche Aufwand nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung der VvFw steht.

Bei der Risikobehandlung ist zudem sicherzustellen, dass die zu ergreifenden Maßnahmen geeignet sind, d.h., dass sie wirken und dass mittels einer maßnahmenspezifischen Bewertung das Risiko unerwünschter Nebeneffekte erkannt und im nächsten Schritt minimiert wird.

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 werden mit Sicherheits-Updates und –Patches ausgestattet.

Bei der Erbringung der VvFw kommt branchenspezifische Technik insbesondere auf den Leitwarten durch spezielle Leittechnik-Software zum Einsatz. Je nach spezifischer Implementierung sind überwiegend 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)

4.2 Allgemeine Anforderungen und Maßnahmen zur Sicherstellung der Informationssicherheit

4.2.1 Implementierung eines Informationssicherheitsmanagementsystems (ISMS)

Im Betrieb des ISMS in Anlehnung an ISO/IEC 27001:2013 müssen die in diesem Dokument beschriebenen Vorgehensweisen und Randbedingungen beachtet werden, damit ein geeigneter Rahmen für die nachhaltige und angemessene Behandlung aller relevanten Risiken und Themenfelder zur Umsetzung der Anforderungen nach § 8a Abs. 1 BSIG gesetzt wird.

Maßgebliche Regelungen und Vorgaben des ISMS sind schriftlich zu dokumentieren. 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.

In Anlehnung an die Norm ISO/IEC 27001:2013 ist Informationssicherheit und deren Weiterentwicklung 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.

4.2.2 Externe Informationsbeschaffung 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 eine geeignete Verfahrensweise zur Beschaffung und Verarbeitung von externen und internen sicherheitsrelevanten Informationen 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.

4.2.3 Steuerung von Lieferanten, Dienstleistern und Dritten

Es müssen dokumentierte Verfahrensweisen existieren, um Lieferanten, Dienstleister und Dritte auf die Einhaltung der geltenden Informationssicherheitsanforderungen (betreffend die für die Funktionsfähigkeit der VvFw maßgeblichen IT) zu verpflichten, sowie diese zu steuern und zu überwachen. Zudem sind alle Lieferungen von und Dienstleistungen an,, informationstechnischen Systemen, Komponenten und Prozessen die für die Funktionsfähigkeit der VvFw maßgeblich sind, zu prüfen:

- wenn informationstechnische Systeme oder Komponenten von Lieferanten bezogen werden oder
- Dienstleister in den Betrieb der VvFw oder die Wartung von hierfür relevanten informationstechnischen Systemen oder Komponenten eingebunden werden.

Beispiele für geeignete Maßnahmen zum Umgang mit Lieferanten und Dienstleistern siehe DIN ISO/IEC 27002 Normenpunkte 15.1.1, 15.1.2, 15.1.3, 15.2.1 und 15.2.2.

4.2.4 Vorfall-, Notfall- und Krisenmanagement

Zur Risikoprävention und –behandlung sind geeignete Prozesse für die Vorfallserkennung und -bearbeitung zur Detektion von Angriffen, Detektion von sonstigen IT-Vorfällen/Störungen und Unterscheidung von Angriffen, zur Reaktion auf Angriffe sowie Reaktion auf sonstige IT-Vorfälle/Störungen zu definieren.

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

Die Prozesse des Notfall- und Krisenmanagements werden in regelmäßigen Abständen überprüft, um ihre Wirksamkeit sowie Umsetzbarkeit in schwierigen Situationen sicherzustellen.

Beispiele für geeignete Maßnahmen zum Vorfall-, Notfall- und Krisenmanagement siehe DIN ISO/IEC 27002 Normenpunkte 17.1.1, 17.1.2, 17.1.3, und 16.

4.2.5 Überprüfung im laufenden Betrieb und Übungen

Die Wirksamkeit der getroffenen Maßnahmen zum Schutz der für die Funktionsfähigkeit der VvFw maßgeblichen informationstechnischen Systeme, Komponenten und Prozesse, muss regelmäßig in geeigneter Weise überprüft werden. Diese Überprüfungen sollten z.B. in spezifischen Audits im Rahmen von Instandhaltungsmaßnahmen oder Prüfungen in Teilbereichen stattfinden. Sie sollten auch außerhalb des von §8a (3) BSIG vorgegebenen Prüfzyklus und Prüfumfangs durchgeführt werden. Hierzu gehören:

- anlassbezogene Prüfungen aufgrund von
  - Änderungen der Bedrohungslage / Gefährdungslage
  - nicht zuverlässig erklärbaren Beeinträchtigungen der für die Funktionsfähigkeit der VvFw maßgeblichen informationstechnischen Systeme oder Komponenten
  - erfolgreichen oder potenziell erfolgreichen Angriffen
  - Änderungen an den für die Funktionsfähigkeit der VvFw maßgeblichen IT- oder Kommunikationssystemen
- Prüfungen in anderen, anderweitig vorgegebenen Prüfzyklen
- Separat finden anlassbezogen Übungen statt:
  - interne Übungen
  - Übungen mit externen Partnern, insbesondere aus dem Kontext der VvFw

4.3 Spezifische Maßnahmen zur Behandlung der unter Punkt 3.3.2 aufgeführten IT-relevanten Gefährdungen

Für einen adäquaten Schutz von Informationen und informationsverarbeitenden Systemen müssen alle im Kapitel 4.2 und 4.3 beschrieben Maßnahmen umgesetzt werden oder Alternativen zum Schutz der für die Funktionsfähigkeit der VvFw maßgebliche IT beschrieben sein. Die Zuordnung der Maßnahmen zu den jeweiligen Risikogruppen dient der strukturierten und systematischen Bearbeitung und Behandlung der Risikofelder.

4.3.1 Maßnahmen zu 1: Physikalische Beeinträchtigung durch Naturgefahren

Zum Schutz der für die Funktionsfähigkeit der VvFw maßgeblichen IT-Systeme müssen bauliche (physische) Sicherheitsvorkehrungen vor Naturkatastrophen oder anderen umweltbedingten Beeinträchtigungen entsprechend der Risikobewertung konzipiert und getroffen werden. Hierzu sind insbesondere folgende Sicherheitsaspekte 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)

Beispiele für geeignete Maßnahmen zum Schutz vor physikalische Beeinträchtigung durch Naturgefahren siehe Normenpunkte 11.1.4 und 11.2.1 der DIN ISO/IEC 27002.

4.3.2 Maßnahmen zu 2: Unterbrechung der Stromversorgung

Soweit IT- Systeme zur Steuerung der Pumpen und Leitsysteme für die Funktionsfähigkeit der VvFw maßgeblich sind, sind diese vor Schäden aufgrund von Stromausfällen zu schützen. Dabei gelten folgende Anforderungen für Stromversorgungseinrichtungen:

- 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 Versorgungseinrichtungen)
- Stromkreise sollten soweit möglich unterteilbar/segmentierbar sein und bei Bedarf mehrere Zuführungen über unterschiedliche Zuleitungswege besitzen
- Stromkabel müssen auf geeignete Weise vor äußerlichen Beeinträchtigungen oder Beschädigungen geschützt sein (möglichst durch unterirdische Verlegung)

Beispiele für geeignete Maßnahmen zum Schutz vor Beeinträchtigungen durch eine Unterbrechung der Stromversorgung siehe Normenpunkte 11.2.2 und 11.2.3 der DIN ISO/IEC 27002.

Weiterhin sind die unter Punkt 4.3.1 aufgeführten Maßnahmen zur Vermeidung von Stromausfällen durch Naturgefahren sicherzustellen.

4.3.3 Maßnahmen zu 3: Zerstörung von Systemen

Die für die Funktionsfähigkeit der VvFw maßgeblichen IT-Systeme müssen angemessen vor Beschädigung oder Zerstörung durch vorsätzliche Angriffe oder Unfälle geschützt werden. Folgende Maßnahmen sind zu betrachten:

- Das Betriebsgelände ist sichtbar und rechtlich eindeutig durch physische Barrieren zu begrenzen, um unberechtigtes Eindringen auf das Betriebsgelände zu erschweren (Zäune, Mauern, einbruchshemmende Türen und Fenster etc.).
- Um zu gewährleisten, dass nur für den Zutritt berechtigte Personen auf das Betriebsgelände gelangen können, ist eine wirksame Zutrittskontrolle einzurichten.
- 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)
- Aufbau von Systemen nach dem “Prinzip der Redundanz” (redundancy principle) – Mithilfe eines geeigneten redundanten Systemdesigns sollen Fehlfunktionen beim Ausfall einzelner informationstechnischer Komponenten kompensiert werden

Beispiele für geeignete Maßnahmen zum Schutz vor Zerstörung von Systemen siehe Normenpunkte 11.1.1, 11.1.2, 11.1.3, 11.1.4, 11.1.5, 11.1.6, 11.2.1, 11.2.6 sowie 17.2.1 der DIN ISO/IEC 27002. Diese sind zu berücksichtigen.

Weiterhin sind die unter Punkt 4.3.1 aufgeführten Maßnahmen zur Vermeidung von Zerstörung von Systemen durch Naturgefahren sicherzustellen.

4.3.4 Maßnahmen zu 4: Ausfall von Systemen/Services

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

Zur Minimierung von Fehlfunktionen der für die Funktionsfähigkeit der VvFw maßgeblichen IT die sowohl vorsätzlich als auch nicht-vorsätzlich ausgelöst werden können, muss eine Architektur (Zonenmodell) verwendet werden, die eine Trennung der kritischen Systeme zur Anlagensteuerung von anderen Systemen und dem Extranet (Internet) vorsieht. Der Zugriff auf die kritischen Systeme findet über sogenannte Sicherheitsgateways statt.

Mit folgenden Prinzipien wird die IT-Architektur der für die Funktionsfähigkeit der VvFw maßgeblichen IT-Systeme gegen vorsätzlich oder unbeabsichtigt herbeigeführte Fehlfunktionen resistent gehalten:

- “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.

Die Architektur eines geeigneten Zonenmodells kann für eine adäquate Umsetzung wie folgt gestaltet sein:

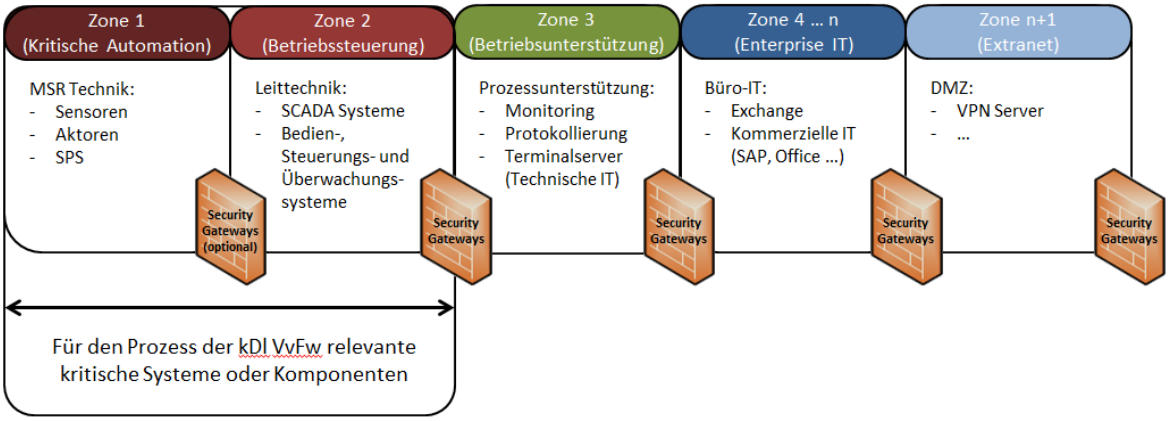

Abb.3 : Architektur Zonenmodell

Weitere technische Beispiele für einen geeigneten Netzwerkschutz finden sich in nachfolgend genannten Abschnitten des „VGB-Standard IT-Sicherheit für Erzeugungsanlagen (VGB-S-175-00-2014-04-DE)“:

- 2.3.1.1: IT-Netztrennung und Segmentierung
- 2.3.1.3: Absicherung Fernzugriffe
- 2.3.2/2.3.2.6: Härtung und sichere Basiskonfiguration der Systeme & Anwendungen
- 2.3.2.5: Schutz vor Schadsoftware
- 2.3.2.9: Intrusion Detection/Prevention
- 2.3.2.7: Kryptographische Absicherung
- 2.3.1.3: Mobile Sicherheit, Sicherheit Mobiler Zugang und Telearbeit
- 2.3.3.2: Datensicherung und Datenwiederherstellung

Beispiele für geeignete Maßnahmen zum Schutz vor Ausfall von Systemen oder Services siehe auch Normenpunkte 10.1.1, 10.1.2, 12.2, 12.3, 12.6, 13.1.1, 13.1.2, 13.1.3 und 13.2.3 der DIN ISO/IEC 27002.

Weiterhin sind die unter 4.3.1 und 4.3.3 aufgeführten Maßnahmen zum Schutz vor physischem Zugang und Umwelteinflüssen zu beachten.

4.3.5 Maßnahmen zu 5: Ausspähen von / Unberechtigter Zugriff auf Daten

Um Daten und Informationen vor unberechtigtem Zugriff oder Ausspähen zu schützen, sind im Unternehmen Grundsätze und Regelungen zur Informationsklassifikation und -handhabung zu beschreiben. Die Klassifizierung von Informationen gemäß gesetzlicher Anforderungen, ihrer Werte und ihrer Kritikalität dient dazu, grundlegende Sicherheitsmaßnahmen für den Schutz von Informationen sowie Anweisungen für deren Handhabung festzulegen. 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 entsprechend gehandhabt werden.

Beispiele zur Informationsklassifizierung und Handhabung finden sich in den Normenpunkten 8.2.1, 8.2.2, 8.2.3, 8.3.1, 8.3.2 und 8.3.3, 18.1.3 und 18.1.4 der DIN ISO/IEC 27002. Diese sind zu berücksichtigen.

Der Zugriff auf Informationen und informationsverarbeitende Systeme ist auf ein Mindestmaß zu beschränken und aktiv über ein Benutzer- und Zugriffsrechtemanagement zu verwalten, zu kontrollieren 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 Passwort. Vorgaben und Beispiele für eine geeignetes Zugriffs- und Netzwerksicherheitsmanagement siehe Normenpunkte 9, 13.1.1 und 13.1.3 der DIN ISO/IEC 27002. Diese sind zu berücksichtigen.

Bei der Verwendung von mobilen Datenträgern (CDs, USB-Sticks, externe Festplatten etc.) ist deren Nutzung gemäß ihrer Klassifikation auf die Befugten und Berechtigten zu beschränken.

Nicht mehr benötigte Informationen und Datenträger sind entsprechend ihrer Klassifizierung 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 den Vorschriften der DIN 32757-1 Norm erfolgen. Beispiele zur sicheren Entsorgung und Weiterverwendung von Betriebsmitteln siehe Normenpunkt 11.2.7 der DIN ISO/IEC 27002.

Weiterhin sind die unter 4.3.3 aufgeführten Maßnahmen zum physischen Zugangsschutz zu beachten.

4.3.6 Maßnahmen zu 6: Missbrauch & Veränderung von Daten

Zur Absicherung gegen Missbrauch & Veränderung von Daten sind insbesondere die unter 4.3.3 aufgeführten Maßnahmen zum physischen Zugangsschutz sowie die unter 4.3.5 aufgeführten Maßnahmen zum Schutz vor Ausspähen von Daten sowie unberechtigtem Zugriff auf Daten zu beachten.

4.3.7 Maßnahmen zu 7: Verlust und Offenlegung von Daten

Zum Schutz vor Verlust von Daten 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.

Ferner 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). Beispiele für eine geeignete Informationssicherung sind unter Normenpunkt 12.3 und 17.2 der DIN ISO/IEC 27002 aufgeführt.

Weiterhin sind die unter 4.3.1 aufgeführten Maßnahmen zum Schutz vor Umwelteinflüssen zu beachten.

4.3.8 Maßnahmen zu 8: Missbrauch & Fälschung von Berechtigungen

:

Um die Möglichkeit zu reduzieren, missbräuchlich Änderungen an Daten vorzunehmen auf die jemand berechtigten Zugriff, sind miteinander in Konflikt stehende Aufgaben- und Verantwortlichkeitsbereiche voneinander zu trennen.

Um die Möglichkeit zu reduzieren, unbefugt Änderungen an oder Fälschungen von Berechtigungen vorzunehmen, dürfen nur Administratoren solche Änderungen vornehmen (entsprechend des Berechtigungskonzeptes).

Beispiele hierfür siehe Normenpunkt 6.1.2 der DIN ISO/IEC 27002.Weiterhin sind insbesondere die unter Punkt 4.3.5 aufgeführten Maßnahmen zum Schutz vor dem Ausspähen von Daten sowie unberechtigtem Zugriff auf Daten zu beachten.

4.3.9 Maßnahmen zu 9: Abstreiten von Aktionen

Um zu verhindern, dass Aktionen abgestritten werden und dadurch nicht mehr nachvollziehbar sind, sind geeignete Maßnahmen zur Dokumentation von Handlungen sowie Informations- und Systemzugriffen einzurichten. Es müssen mindestens folgende Ereignisse protokolliert werden:

- Ausnahmen von geltenden Richtlinien und Anweisungen
- Informationssicherheitsvorfälle

Protokollierungseinrichtungen und/oder -Systeme sowie Aufzeichnungen und Nachweise sind vor Manipulation und unbefugtem Zugriff geschützt aufzubewahren. Insbesondere bei Ausnahmen ist zudem die Notwendigkeit zu deren Fortbestehen regelmäßig nachzuprüfen.

Beispiele zur Nachvollziehbarkeit von Tätigkeiten sind in der DIN ISO/IEC 27002 unter den Normenpunkten 12.4 aufgeführt.

4.3.10 Maßnahmen zu 10: Manipulation an Software

Zur Absicherung gegen Manipulation an Software sind insbesondere die unter 4.3.3 aufgeführten Maßnahmen zum physischen Zugangsschutz sowie die unter 4.3.5 aufgeführten Maßnahmen zum Schutz vor Ausspähen von Daten sowie unberechtigtem Zugriff auf Daten zu beachten.

4.3.11 Maßnahmen zu 11: Fehlerhafte Software, Firmware & Hardware

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

- Regeln für die Installation von Software durch Benutzer festzulegen und umzusetzen
- Verfahrensweisen zur Steuerung von Softwareinstallationen auf im Betrieb befindlichen Systemen zu definieren und zu implementieren.

Zudem ist ein wirksames Änderungsmanagement zu etablieren, welches folgende Aspekte beinhaltet:

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

Beispiele zur Absicherung gegen fehlerhafte Software, Firmware und Hardware sind in der DIN ISO/IEC 27002 unter den Normenpunkten 12.5.1, 12.6.1 sowie 14.2 aufgeführt.

4.3.12 Maßnahmen zu 12: Fehlerhafte Administration von Systemen

Zur Verhinderung von fehlerhafter Administration von Systemen ist sicherzustellen, dass erforderliche Bedien- und Betriebsabläufe dokumentiert sind und den Nutzern, die sie benötigen, zur Verfügung stehen. Geeignete Dokumentationsformen sind z.B. in der DIN ISO/IEC 27002 unter Normenpunkt 12.1.1 beschrieben.

Weiterhin ist im Rahmen des Personalmanagements darauf zu achten, dass Administratortätigkeiten nur von ausreichend qualifiziertem Personal wahrgenommen werden. Alle Beschäftigten des Unternehmens sowie Dienstleister und Auftragnehmer, die Tätigkeiten an IT Systemen, die für die Funktionsfähigkeit der VvFw maßgeblich sind, durchführen, sind regelmäßig zu den, für ihr berufliches Arbeitsgebiet relevanten, geltenden Richtlinien und Verfahren des Unternehmens zu schulen bzw. zu unterweisen. Für Beispiele zur Personalqualifizierung siehe auch DIN ISO/IEC 27002 Normenpunkt 7.2.2.

Zusätzlich sind die unter 4.3.9 aufgeführten Maßnahmen zur Nachvollziehbarkeit von Tätigkeiten zu beachten.

4.3.13 Maßnahmen zu 13: Fehlerhafte Bedienung von Systemen

Zur Vermeidung von fehlerhafter Bedienung von IT Systemen, die für die Funktionsfähigkeit der VvFw maßgeblich sind, sind die unter Punkt 4.3.12 aufgeführten Maßnahmen zur Verhinderung von fehlerhafter Administration von Systemen umzusetzen.

Weiterhin ist im Rahmen des Personalmanagements darauf zu achten, dass Bedien- und Benutzeraktivitäten nur von ausreichend qualifiziertem Personal durchgeführt werden. Alle Beschäftigten des Unternehmens sowie Dienstleister und Auftragnehmer, die Tätigkeiten an IT Systemen, die für die Funktionsfähigkeit der VvFw maßgeblich sind, durchführen, sind regelmäßig zu den, für ihr berufliches Arbeitsgebiet relevanten, geltenden Richtlinien und Verfahren des Unternehmens zu schulen bzw. zu unterweisen. Für Beispiele zur Personalqualifizierung siehe auch DIN ISO/IEC 27002 Normenpunkt 7.2.2 und 12.1.1.

4.3.14 Maßnahmen zu 14: Nichtautorisierte Nutzung von Daten oder Software

Zum Schutz gegen eine nichtautorisierte Nutzung von Daten oder Software sind insbesondere die unter 4.3.3 aufgeführten Maßnahmen zum physischen Zugangsschutz sowie die unter 4.3.5 aufgeführten Maßnahmen zum Schutz vor dem Ausspähen von Daten sowie unberechtigtem Zugriff auf Daten zu beachten.

Zudem ist eine robuste bzw. resiliente Architektur, wie in Kapitel 4.3.4 beschrieben, zu berücksichtigen.

4.3.15 Maßnahmen zu 15: Verwendung von Daten oder Software aus nicht vertrauenswürdigen Quellen

Im Rahmen des ISMS muss in Informationssicherheitsrichtlinien der Umgang mit sowie die Verwendung von Informationen, Systemen und Software beschrieben und geregelt sein.

Weiterhin gelten die Maßnahmen des Kapitels 4.3.11 zur Vermeidung der Verwendung fehlerhafter Software, Firmware & Hardware.

4.3.16 Maßnahmen zu 16: Diebstahl von Medien oder Dokumenten

Zum Schutz vor Diebstahl sind insbesondere die unter 4.3.3 aufgeführten Maßnahmen zum physischen Zugangsschutz umzusetzen.

Weiterhin muss die Mitnahme bzw. das Entfernen von Geräten, Betriebsmitteln, Informationen oder Software geregelt sein und geeignet dokumentiert werden.

4.3.17 Maßnahmen zu 17: Zerstörung oder Ausfall von Ausrüstung oder Medien

Zum Schutz vor Zerstörung von Medien sind die unter 4.3.1 und 4.3.3 aufgeführten die Maßnahmen zum Schutz vor physischem Zugang und Umwelteinflüssen umzusetzen.

Um einem Ausfall von Medien entgegenzuwirken oder zu kompensieren, gelten die Schutzmaßnahmen des Kapitels 4.3.4 „Ausfall von Systemen/Services“.

4.3.18 Maßnahmen zu 18: Nichtautorisierte Nutzung von Ausrüstung

Es gelten die Maßnahmen des Kapitels 4.3.14 „Nichtautorisierte Nutzung von Daten oder Software“.

4.3.19 Maßnahmen zu 19: Diebstahl von Ausrüstung

Es gelten die Maßnahmen des Kapitels 4.3.16 „Diebstahl von Medien oder Dokumenten“.

4.3.20 Maßnahmen zu 20: Schadcode wird in Systeme eingebracht

Um zu vermeiden, dass Schadcode in IT-Systeme, die für die Funktionsfähigkeit der VvFw maßgeblich sind, eingebracht wird und negative Auswirkungen verursacht, sind geeignete technische und organisatorische Schutzmaßnahmen umzusetzen und die unter 4.3.3 aufgeführten Maßnahmen zum physischen Zugangsschutz zu beachten:

Beispiele zum Schutz vor Schadcode finden sich in der DIN ISO/IEC 27002 unter den Normenpunkten 12.2.1 und 12.6.1.

4.3.21 Maßnahmen zu 21: Verletzung der Instandhaltbarkeit von Informationssystemen

Um die ordnungsgemäße Verfügbarkeit und Integrität von IT-Systemen, die für die Funktionsfähigkeit der VvFw maßgeblich sind, zu gewährleisten, müssen diese fortlaufend instand gehalten werden. Um dies sicherzustellen, müssen:

- diese Unternehmenswerte in einem Inventar erfasst und gepflegt werden
- diesen Unternehmenswerten eindeutige Verantwortlichkeiten zugewiesen werden.

Weiterführende Beispiele zur Sicherstellung der Instandhaltbarkeit von Informationssystemen finden sich in der DIN ISO/IEC 27002 unter den Normenpunkten 8.1, 11.2.4, sowie 12.1.

Zudem sind die unter Punkt 4.3.11 aufgeführten Maßnahmen zum Änderungsmanagement zu berücksichtigen.

4.3.22 Maßnahmen zu 22: Nichtverfügbarkeit von Personal

Um zu vermeiden, dass eine Nichtverfügbarkeit von Personal zur Beeinträchtigung oder Ausfall der IT-Systeme, die für die Funktionsfähigkeit der VvFw maßgeblich sind, führt, sind folgende präventive Maßnahmen umzusetzen:

Die Unternehmensleitung bekennt sich aktiv zur Informationssicherheit und verlangt von allen Beschäftigten und Auftragnehmern die Einhaltung und Umsetzung der eingeführten Richtlinien und Verfahren.

Verantwortlichkeiten und Pflichten im Bereich der Informationssicherheit sind festgelegt und zugeordnet sowie den Mitarbeitern bekannt gemacht.

Für Beispiele zur Vermeidung von Beeinträchtigungen durch die Nichtverfügbarkeit von Personal siehe DIN ISO/IEC 27002 Normenpunkte 5.1.1, 5.1.2, 6.1.11 , 7.1.2, 7.2 sowie 7.3.1.

4.3.23 Maßnahmen zu 23: Bestechung oder Betrug

Um die Gefahr von Bestechung und Korruption zu reduzieren, sind Aufgaben, Pflichten und Verantwortlichkeiten, die zu Interessenskonflikten führen können, zu trennen. Weiterhin müssen wirksame Kontrollmechanismen zur Überprüfung und Aufrechterhaltung der Informationssicherheit in allen Geschäftsprozessen etabliert sein sowie in regelmäßigen Abständen auf ihre fortbestehende Wirksamkeit geprüft werden.

Als Beispiel siehe DIN ISO/IEC 27002, Normenpunkt 7.

Zudem sind insbesondere die Maßnahmen der Kapitel 4.3.9 „Abstreiten von Aktionen“, 4.3.6/8 „Missbrauch & Veränderung von Daten/Berechtigungen“ sowie 4.3.12/13 „Fehlerhafte Administration/Bedienung von Systemen“ einzuhalten.

4.3.24 Maßnahmen zu 24: Nichteinhaltung von Vorgaben

Es ist ein formal festgelegter und bekanntgegebener Maßregelungsprozess zu etablieren, um Informationssicherheitsverstöße zu ahnden.

Als Beispiel siehe DIN ISO/IEC 27002, Normenpunkt 7.2.3.

4.3.25 Maßnahmen zu 25: Nichtverfügbarkeit von Betriebsstätten

Um einer Nichtverfügbarkeit von Betriebsstätten entgegenzuwirken, sind die unter Punkt 4.3.1 und 4.3.3 aufgeführten Maßnahmen zum Schutz vor Umwelteinflüssen und physischen Zutrittsschutz zu beachten.

Um eine Verfügbarkeit der Betriebsstätten auch in allgemeinen Krisenlagen sicherzustellen, sind zudem die Maßnahmen des Kapitels 4.2.4 „Vorfall-, Notfall- und Krisenmanagement“ umzusetzen.

5 Nachweisbarkeit der Umsetzung

Zur Erfüllung der Anforderungen gemäß § 8a Absatz 1 BSIG muss mindestens alle zwei Jahre geprüft und nachgewiesen werden, dass zur Absicherung der für die Funktionsfähigkeit der VvFw maßgeblichen IT ein ISMS gemäß dem B3S oder adäquate Schutzvorkehrungen vorhanden sind, und dass die getroffenen Maßnahmen dem Stand der Technik entsprechen.

Als Nachweis eignet sich z.B. ein Zertifizierungs- oder Prozessaudit, bei dem die informationstechnischen Systeme, die für die Funktionsfähigkeit der VvFw maßgeblich sind, bezüglich der Einhaltung der Schutzziele betrachtet und untersucht werden. Als Grundlage für jedes Prüfschema sollten international anerkannte Standards oder Regeln dienen, wie z.B. die verbindlichen Bewertungsgrundlagen für Audits und Zertifizierungen der „International Organization for Standardization (ISO)“ oder branchenspezifische Vorgaben von Industriezweigen oder Dienstleistungsbereichen. Einen Leitfaden zur Erfüllung und Nachweisbarkeit der gesetzlichen Anforderungen liefert auch die „Orientierungshilfe zu Nachweisen gemäß § 8a (3) BSIG“.

Geeignete prüfende Stellen:

Im Audit wird die Konformität mit diesem B3S überprüft und offiziell mit einem Dokument bestätigt. Wesentliche Voraussetzung für die Nachweiserbringung ist die unabhängige, unparteiliche und objektive Bewertung durch eine dritte, kompetente Stelle. Diese Funktion kann nach Wahl des Betreibers ein interner Revisor, ein Wirtschaftsprüfer oder ein externer Auditor mit branchenspezifischer Expertise im Energiesektor sowie der AGFW übernehmen.

Kompetenznachweis des Auditors:

Für die Nachweisprüfung nach §8a BSIG sind entsprechende Prüfverfahrens-Kompetenzen nötig, d.h. die Prüfer müssen mindestens eine Qualifikation zu den Prüfvorgaben und Anforderungen aus dem „B3S VvFw“ besitzen, sowie über IT-Kompetenz und über branchenspezifische Expertise im Energiesektor verfügen.

Prüfumfang und -dauer:

Der Prüfumfang und die Prüfdauer werden in Anlehnung an die Vorgaben der ISO/IEC 17021-1:2015 durch den Auditor festgelegt. Sowohl Umfang als auch Dauer richten sich grundsätzlich nach der Größe des Geltungsbereiches.

Der Auditor hat innerhalb eines Nachweiszyklus stichprobenartig alle unter den Anwendungsbereich fallenden informationstechnischen Systeme und Komponenten und Prozesse, die für die Funktionsfähigkeit der VvFw maßgeblich sind, auf Einhaltung der Schutzziele zu überprüfen. Es ist zulässig, bei der Auditierung eine Stichprobe der Standorte zu wählen, bzw. Betriebsstätten durch geeignete Gruppenbildung zusammenzufassen. Bei der Wahl der Stichproben ist darauf zu achten, dass in der Gesamtheit der Stichproben eine gute netztopologische Abdeckung erzielt wird, also auch geographisch möglichst viele Teile des Scopes berücksichtigt werden.

Der KRITIS Betreiber übermittelt dem BSI als Nachweis die Ergebnisse der durchgeführten Prüfungen oder Zertifizierungen inklusive der Liste der dabei aufgedeckten Sicherheitsmängel.

Literaturverzeichnis

DIN ISO/IEC 27001:2013 (inkl. Cor.1:2014 & Cor. 2:2015)	Original-Titel (Englisch): *Information technology - Security techniques - Information security management systems - Requirements* Titel (Deutsch) *IT-Sicherheitsverfahren – Informationssicherheits-Managementsysteme – Anforderungen*
DIN ISO/IEC 27002:2013 (inkl. Cor.1:2014 & Cor. 2:2015)	Original-Titel (Englisch): *Information technology - Security techniques - Code of practice for information security controls* Titel (Deutsch) *Informationstechnik - Sicherheitsverfahren - Leitfaden für Informationssicherheitsmaßnahmen*
VGB-S-175-00-2014-04-DE	Technischer Standard des VGB PowerTech Titel (Deutsch) *IT-Sicherheit für Erzeugungsanlagen*
Orientierungshilfe zu Nachweisen gemäß § 8a (3) BSIG	Bundesamt für Sicherheit in der Informationstechnik Version 0.9.02 vom 30.06.2017