ABSCHLUSSBERICHT AP 12
GESTALTUNG UND NUTZUNG VON
SICHERHEITSKONZEPTEN UND STANDARDISIERUNG

2021

enera

Inhalte

IT-Grundschutz-Profil Virtuelles Kraftwerk 3

Gesetze, Regularien, Richtlinien, Compliance, Zertifizierungen 71

Governance, Compliance und Datenschutz: Erhebungen, Strukturen und Management 128

Methoden und Verfahren zur Systementwicklung
Anpassungen des Use Case-Templates hinsichtlich Security-by-Design 196

Schulung und Sensibilisierung 250

Incident Handling (IH) 307

Notfallmanagement / Continuity Management 326

Gap-Analyse 342

IT-Grundschutz-Profil Virtuelles Kraftwerk

Autoren:

Rolf Apel (Siemens), Konrad Rosmus (IABG)

17.12.2020

Gefördert durch:

Bundesministerium für Wirtschaft und Energie

aufgrund eines Beschlusses des Deutschen Bundestages

Inhalt

1 Management Summary 4
2 Festlegung des Geltungsbereichs 4

2.1 Zielgruppe 4
2.2 Schutzbedarf 4
2.3 IT-Grundschutzvorgehensweise 5
2.4 Rahmenbedingungen 5

3 Entwicklung des Informationsverbundes basierend auf den Use Cases 6

3.1 Nicht berücksichtigte Objekte 6

4 Referenzarchitektur 7

4.1 Netzplandarstellung 7

4.1.1 High-Level-Darstellung 7
4.1.2 Detaillierte Darstellung 7

4.2 Zielobjekte 9

4.2.1 Infrastruktur 9
4.2.2 Netze und Kommunikation 9
4.2.3 IT-Systeme: 10
4.2.4 Industrielle IT 10
4.2.5 Geschäftsprozesse 10
4.2.6 Anwendungen 11
4.2.7 Beziehungen zwischen den Zielobjekten 11

5 Schutzbedarfsfeststellung 13

5.1 Schutzbedarfskategorien 13
5.2 Vorschläge für Schutzbedarfe 16

5.2.1 Geschäftsprozesse 16
5.2.2 Anwendungen 18
5.2.3 IT-Systeme, ICS-Systeme und sonstige Geräte 20
5.2.4 Infrastruktur 23
5.2.5 Netze und Kommunikationsverbindungen 24

6 Zuordnung der relevanten Bausteine 31

6.1 Zuordnung der relevanten Prozessbausteine 31
6.2 Zuordnung der relevanten Systembausteine 33

7 Sicherheitsanforderungen und umzusetzende Maßnahmen 39
8 Exemplarische Risikoanalyse 40

8.1 Bewertung der Ausgangslage und Bildung von Risikobereichen 40

8.1.1 Bewertung der Ausgangslage 40
8.1.2 Bildung von Risikobereichen aufgrund des Schutzbedarfes 40
8.1.3 Bildung von Risikobereichen aufgrund der Modellierbarkeit 41

8.2 Risikoanalysen 42

8.2.1 Risikobereich „Verlust von Vertraulichkeit (Schwerpunkt), Integrität und Authentizität (besonderer) personenbezogener Daten“ 42
8.2.2 Risikobereich „Verlust der Integrität (Schwerpunkt), Authentizität und Verfügbarkeit von Kontroll- und Steuerungsdaten und -funktionen“ 55
8.2.3 Risikobereich „Vorsätzliche Überwindung oder zufällige Schäden (einschließlich höherer Gewalt) bei Infrastruktureinrichtungen der dezentralen Erzeuger bzw. Verbraucher“ 60

8.3 Schlussfolgerungen aus den Ergebnissen der Schwachstellen-, Bedrohungs- und Risikoanalyse 63

9 Alternativer Ansatz Risikobehandlung: Direkte Zuordnung von Anforderungen aus anderen Standards 63
10 Anwendungshinweise 66
11 Unterstützende Informationen 66
12 Abkürzungsverzeichnis 67

1 Management Summary

Das IT-Grundschutzprofil *Virtuelles Kraftwerk* definiert einen Mindestschutzbedarf für die verarbeiteten Informationen, Verbrauchs- und Erzeugungsdaten, Abrechnungsdaten, Messwerte etc., welche im Betrieb eines virtuellen Kraftwerks zwischen Aktoren ausgetauscht werden, sowie für dazu erforderliche Dienste, Systeme und Infrastrukturkomponenten. Zu deren Absicherung wird, soweit es möglich ist, auf bestehende Bausteine aus dem IT-Grundschutzkompendium zurückgegriffen.

Das IT-Grundschutzprofil richtet sich an Betreiber eines virtuellen Kraftwerks im Smart Grid und soll die verantwortlichen Leitungsebenen, die zuständigen Informationssicherheitsbeauftragten sowie weitere mit Informationssicherheitsaufgaben betraute Personen beim Aufbau eines Managementsystems für Informationssicherheit (ISMS) nach IT-Grundschutz unterstützen. Es kann auch für weitere Parteien, welche mit einem virtuellen Kraftwerk interagieren, von Interesse sein. Dies können beispielsweise Übertragungs- und Verteilnetzbetreiber, Messstellenbetreiber, private und gewerbliche Erzeuger dezentraler erneuerbarer Energieressourcen sowie Verbraucher sein.
Dieses Profil wurde im Rahmen des Teilarbeitspaketes TAP 12.2 „Informationssicherheitskonzept“ im SINTEG-Projekt enera entwickelt. Ausgangspunkt war der aus den enera Use Cases abgeleitete Scope "Virtuelles Kraftwerk". Es weicht in einigen Teilen von den Festlegungen des BSI zu Grundschutzprofilen ab und kann dahingehend von interessierter Seite weitergeführt werden.

2 Festlegung des Geltungsbereichs

2.1 Zielgruppe

Primär Betreiber eines virtuellen Kraftwerks und sekundär alle diejenigen, welche mit einem virtuellen Kraftwerk interagieren.

2.2 Schutzbedarf

Hinsichtlich des Schutzniveaus definiert das vorliegende Profil ein Niveau, das über der Standard-Absicherung der IT-Grundschutzvorgehensweise liegt, da im Umfeld von virtuellen Kraftwerken in der Regel

- Steuerungsdaten für an das elektrische Energieversorgungsnetz angeschlossene Erzeugungsanlagen sowie
- personenbezogenen Abrechnungsdaten, auf deren Vertraulichkeit hoher Wert gelegt wird,

verarbeitet werden. Darüber hinaus besteht meist ein erhöhter Schutzbedarf hinsichtlich der Verfügbarkeit der Steuerungsfunktionen der Erzeugungsanlagen, um bei Netzproblemen schnell und zuverlässig reagieren zu können. Daher ist für personenbezogene Abrechnungsdaten ein Schutzbedarf von „hoch" bezüglich Vertraulichkeit und ggf. Integrität anzunehmen und bei Steuerungsdaten ein „hoch“ bezüglich Verfügbarkeit und Integrität. Diese Schutzbedarfsfeststellung ist bei der Anwendung des IT-Grundschutzprofils zu berücksichtigen.

2.3 IT-Grundschutzvorgehensweise

Die in diesem Profil aufgeführten Anforderungen sind Empfehlungen des Arbeitspakets 12 im SINTEG Projekt enera. Sie decken mindestens die Anforderungen der Standard-Absicherung des BSI-Standards 200-2 ab, teilweise müssen außerdem Anforderungen aus dem Bereich des erhöhten Schutzbedarfs umgesetzt werden.

Abdeckung Vorgehensweise: Mindestens Standard-Absicherung, teilw. erhöhte Absicherung.

ISO 27001-Kompatibilität: ja

2.4 Rahmenbedingungen

Die Anwendung des Profils ist nur in Verbindung mit dem jeweils aktuellen IT-Grundschutzkompendium des BSI möglich. Wegen fehlender Anforderungen in vorhandenen Bausteinen bzw. dem Fehlen ganzer Bausteine im IT-Grundschutzkompendium wurden im Rahmen der Risikoanalyse zusätzliche Anforderungen basierend auf den internationalen Standards IEC 62351 und IEC 62443 hinzugenommen.

3 Entwicklung des Informationsverbundes basierend auf den Use Cases

In Abbildung 1 ist der Informationsverbund des IT-Grundschutzprofils *Virtuelles Kraftwerk* (gelb) basierend auf der Beschreibung der enera Use Cases dargestellt. Die Abbildung ist im Unterschied zum originären Use Case auf die wesentlichen Akteure eines virtuellen Kraftwerks begrenzt. Ebenso sind weitere Bereiche im Umfeld des virtuellen Kraftwerks dargestellt, für welche die Möglichkeit besteht weitere Profile zu entwickeln.
Der Informationsverbund, welchen das vorliegende IT-Grundschutzprofil *Virtuelles Kraftwerk* umfasst, enthält alle Akteure, Prozesse und ausgetauschte Informationen, die für den Standardbetrieb eines virtuellen Kraftwerks notwendig sind.

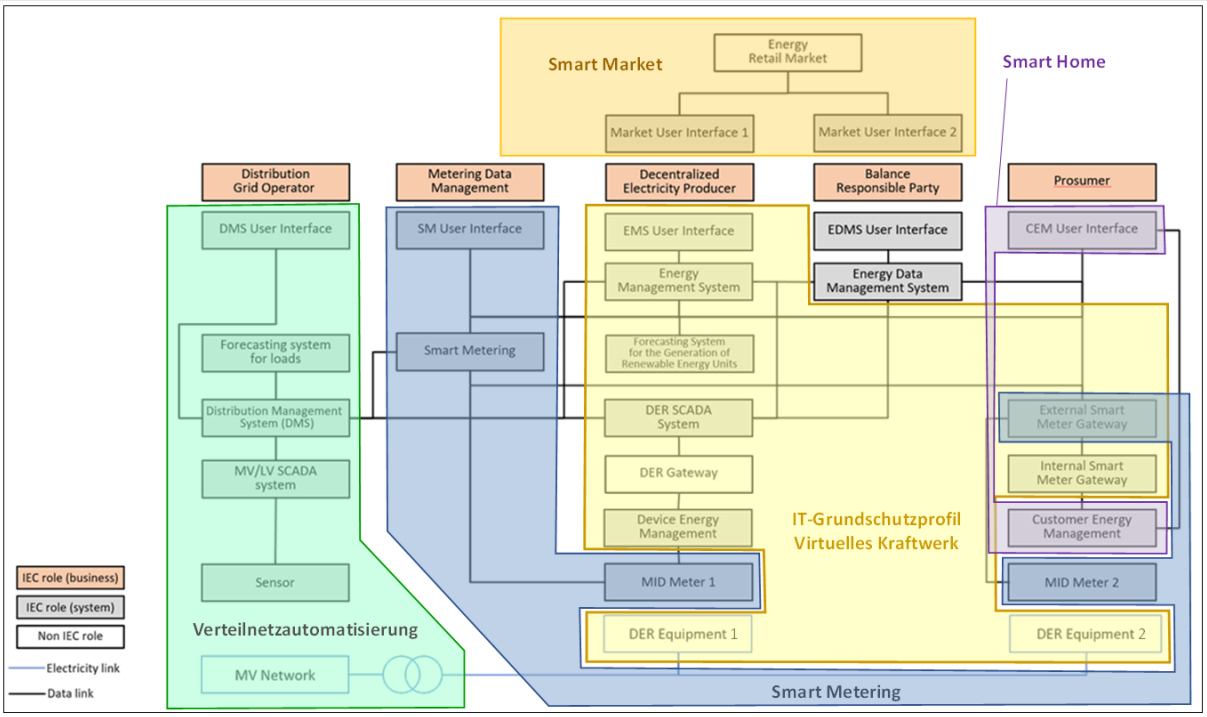


Abbildung 1: Darstellung und Abgrenzung anhand der Use Cases

Zu den Akteuren bzw. korrespondierenden Zielobjekten gehört das *EMS User Interface* sowie das zugehörige *System Energy Management System*. Weiterhin relevant sind das *Forecasting System for the Generation of Renewable Energy Units*, das *DER SCADA System*, ein *DER Gateway* und das *Device Energy Management* sowie analog dazu das *External* und *Internal Smart Meter Gateway*. Als letztendlicher Energieerzeuger gehört auch das *DER Equipment* zum Informationsverbund.
Wie außerdem aus Abbildung 1 ersichtlich ist, bestehen einige Verknüpfungen des Profils zu anderen möglichen Profilen aus dem Umfeld des virtuellen Kraftwerks. Über diese Schnittstellen werden ebenfalls Informationen ausgetauscht.

3.1 Nicht berücksichtigte Objekte

Nicht berücksichtigt werden alle Objekte außerhalb des Profils *Virtuelles Kraftwerk*. Eindeutig abgegrenzt und ausgeschlossen sind insbesondere diejenigen Objekte, welche in Abbildung 1 nicht im gelb hinterlegten Bereich enthalten sind.

4 Referenzarchitektur

4.1 Netzplandarstellung

4.1.1 High-Level-Darstellung

In Abbildung 2 ist der dem IT-Grundschutzprofil zu Grunde liegende Informationsverbund grau hinterlegt dargestellt (MID Meter 1&2, Customer Energy Management, zugehöriges User Interface sowie Market User Interface 1 ausgeschlossen). Ebenso sind alle Schnittstellen an den Grenzen des Informationsverbunds eingezeichnet.

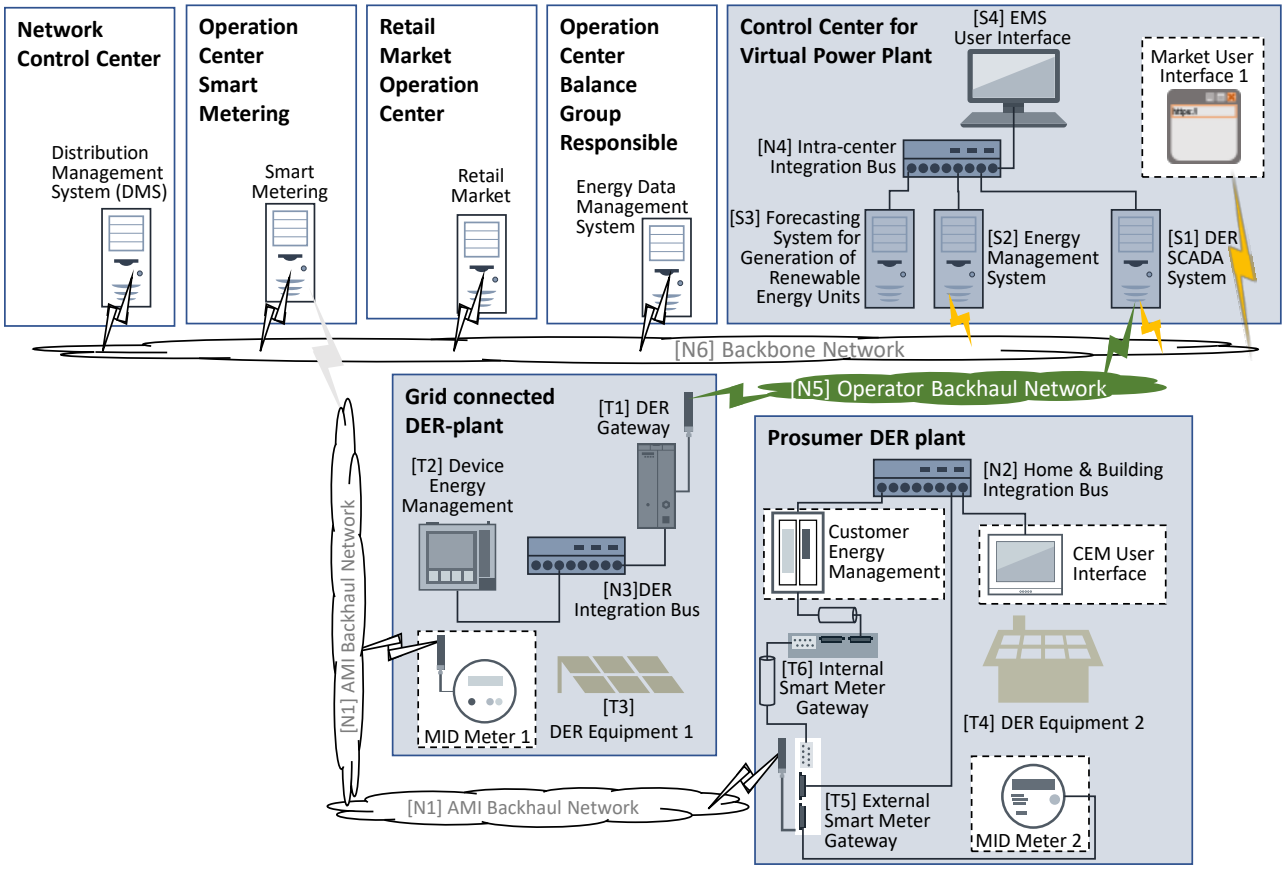


Abbildung 2: High-Level Darstellung des Netzplans

4.1.2 Detaillierte Darstellung

Die detailliertere Darstellung des Netzplans in Abbildung 3 kann als Orientierung zur Erstellung eines konsolidierten Netzplans bei der Anwendung des Grundschutzprofils für ein konkretes virtuelles Kraftwerk dienen.

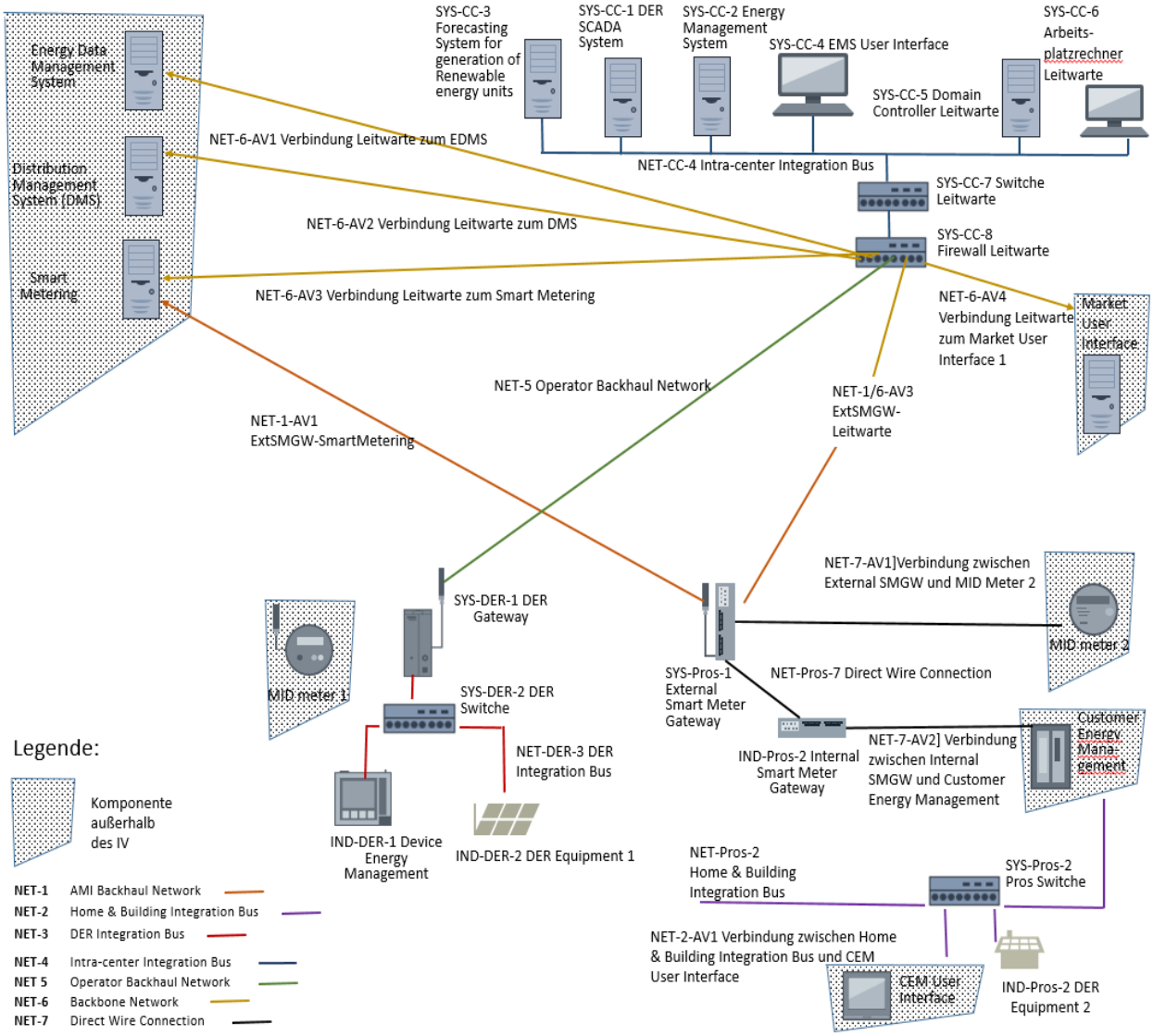


Abbildung 3: Detaillierter Netzplan

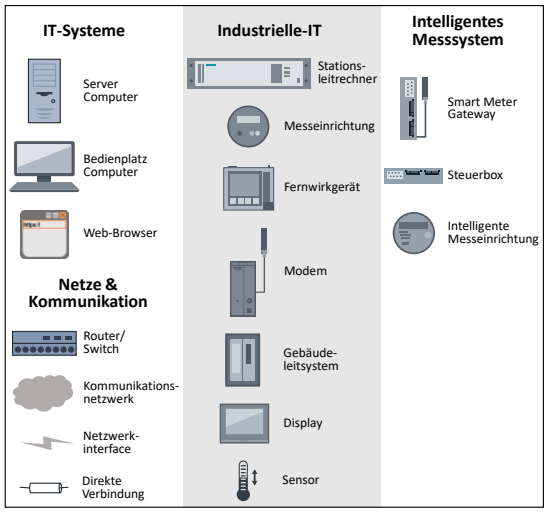


Abbildung 4: Agenda zu Abbildung 2 und Abbildung 3

4.2 Zielobjekte

Die Zielobjekte der Referenzarchitektur sind in die Kategorien Infrastruktur, Netze und Kommunikation, IT-Systeme, industrielle IT sowie Geschäftsprozesse / Anwendungen eingeteilt. Im Folgenden wird die Kategorisierung der Akteure im Informationsverbund vorgenommen.

4.2.1 Infrastruktur

Infrastruktur netzgebundene DER-Anlage / Grid connected DER plant

- [INF-DER-1] Betriebsgelände DER-Anlage (enthält DER Equipment 1, z. B. Photovoltaik)
- [INF-DER-2] Betriebsgebäude DER-Anlage (enthält DER Gateway, Device Energy Management)

Infrastruktur Unternehmen / Control Center for Virtual Power Plant

- [INF-CC-1] Unternehmensgebäude (enthält Serverraum, Wartenraum, Büroräume und Technikräume)
- [INF-CC-2] Serverraum im Unternehmensgebäude (enthält Energy Management System, Forecasting System for the Generation of Renewable Energy Units, DER SCADA System)
- [INF-CC-3] Warteraum im Unternehmensgebäude (enthält EMS User Interface)
- [INF-CC-4] Büroräume im Unternehmensgebäude (enthalten Arbeitsplatzrechner)
- [INF-CC-5] Technikräume im Unternehmensgebäude (enthalten unterstützende Infrastruktur und Versorgungssysteme)

Infrastruktur Prosumer-DER-Anlage / Prosumer DER plant

- [INF-Pros-1] Zählerkasten zur Prosumer-DER-Anlage (z. B. im Wohnhaus; enthält External Smart Meter Gateway, Internal Smart Meter Gateway, Customer Energy Management)
- [INF-Pros-2] Aufstellungsort Prosumer-DER-Anlage (z. B. Dach des Wohnhauses; Aufstellungsort für DER Equipment 2, z. B. Photovoltaik)

4.2.2 Netze und Kommunikation

Außenverbindungen

- [NET-1-AV1] Verbindung External SMGW zum Smart Metering (via AMI Backhaul Network)
- [NET-1/6-AV2] Verbindung External SMGW zur Leitwarte (via AMI Backhaul Network und Backbone Network (realisierungsabhängig, z. B. Internet mit Umsetzer dazwischen))
- [NET-6-AV1] Verbindung Leitwarte zum EDMS (via Backbone Network (z. B. Internet))
- [NET-6-AV2] Verbindung Leitwarte zum DMS (via Backbone Network (z. B. Internet))
- [NET-6-AV3] Verbindung Leitwarte zum Smart Metering (via Backbone Network (z. B. Internet))
- [NET-6-AV4] Verbindung Leitwarte zum Market User Interface 1 (via Backbone Network (z. B. Internet))
- [NET-2-AV1] Verbindung zwischen Home & Building Integration Bus und CEM User Interface (letzteres ist nicht im IV)
- [NET-7-AV1] Verbindung zwischen External SMGW und MID Meter 2 (letzteres ist nicht im IV)
- [NET-7-AV2] Verbindung zwischen Internal SMGW und Customer Energy Management (letzteres ist nicht im IV)

Interne Netze und Verbindungen

- [NET-Pros-2] Home & Building Integration Bus
- [NET-DER-3] DER Integration Bus
- [NET-CC-4] Intra-center Integration Bus
- [NET-5] Operator Backhaul Network
- [NET-Pros-7] Direct Wire Connection

4.2.3 IT-Systeme:

- [SYS-CC-1] DER SCADA System
- [SYS-CC-2] Energy Management System
- [SYS-CC-3] Forecasting System for the Generation of Renewable Energy Units
- [SYS-CC-4] EMS User Interface
- [SYS-CC-5] Domain Controller Leitwarte
- [SYS-CC-6] Arbeitsplatzrechner Leitwarte
- [SYS-CC-7] Switche Leitwarte
- [SYS-CC-8] Firewall Leitwarte

- [SYS-DER-1] DER Gateway
- [SYS-DER-2] DER Switche

- [SYS-Pros-1] External Smart Meter Gateway
- [SYS-Pros-2] Pros Switche

4.2.4 Industrielle IT

- [IND-DER-1] Device Energy Management
- [IND-DER-2] DER Equipment 1

- [IND-Pros-1] Internal Smart Meter Gateway
- [IND-Pros-2] DER Equipment 2

4.2.5 Geschäftsprozesse

- [PROZ-1] Standardbetrieb (Planung und Steuerung) des virtuellen Kraftwerks
- [PROZ-2] Netzüberlast und Abschaltung der DER Energieerzeugung
- [PROZ-3] Abrechnung von Verbrauchs- / Erzeugerdaten
- [PROZ-4] Bereitstellung von Regelenergie
- [PROZ-5] Bereitstellung von Energie und Handel an der Strombörse

4.2.6 Anwendungen

- [ANW-1] Energie Managementsystem
- [ANW-2] Vorhersagesystem
- [ANW-3] Kontroll- und Steuerungssystem
- [ANW-4] Netzdienste, Benutzer- und Ressourcenverwaltung
- [ANW-5] Büroanwendungen

4.2.7 Beziehungen zwischen den Zielobjekten

Zuordnung Anwendungen zu Geschäftsprozessen:

	[PROZ-1]	[PROZ-2]	[PROZ-3]	[PROZ-4]	[PROZ-5]
[ANW-1] Energie Managementsystem			x		
[ANW-2] Vorhersagesystem	x	x			
[ANW-3] Kontroll- und Steuerungssystem	x	x		x	x
[ANW-4] Netzdienste, Benutzer- und Ressourcenverwaltung	x	x	x	x	x
[ANW-5] Büroanwendungen			x		

Tabelle 1: Zuordnung Anwendungen zu Geschäftsprozesse

Zuordnung Anwendungen zu Systemen:

	[ANW-1]	[ANW-2]	[ANW-3]	[ANW-4]	[ANW-5]
[SYS-CC-1] DER SCADA System			x		
[SYS-CC-2] Energy Management System	x				
[SYS-CC-3] Forecasting System for the Generation of Renewable Energy Units		x			
[SYS-CC-4] EMS User Interface	x				
[SYS-CC-5] Domain Controller Leitwarte				x	
[SYS-CC-6] Arbeitsplatzrechner Leitwarte					x
[SYS-CC-7] Switche Leitwarte				x	
[SYS-CC-8] Firewall Leitwarte				x	
[SYS-DER-1] DER Gateway			x		
[SYS-DER-2] DER Switche				x	
[SYS-Pros-1] External Smart Meter Gateway			x		
[SYS-Pros-2] Pros Switche				x	
[IND-DER-1] Device Energy Management			x		
[IND-DER-2] DER Equipment 1			x		
[IND-Pros-1] Internal Smart Meter Gateway			x		
[IND- Pros -2] DER Equipment 2			x		

Tabelle 2: Zuordnung Anwendungen zu Systemen

Zuordnung Systeme zu Infrastruktur:

	INF-DER-1	INF-DER-2	INF-CC-1	INF-CC-2	INF-CC-3	INF-CC-4	INF-CC-5	INF-Pros-1	INF-Pros-2
[SYS-CC-1] DER SCADA System				x					
[SYS-CC-2] Energy Management System				x					
[SYS-CC-3] Forecasting System for the Generation of Renewable Energy Units				x					
[SYS-CC-4] EMS User Interface					x				
[SYS-CC-5] Domain Controller Leitwarte				x					
[SYS-CC-6] Arbeitsplatzrechner Leitwarte						x			

[SYS-CC-7] Switche Leitwarte				x					
[SYS-CC-8] Firewall Leitwarte				x					
[SYS-DER-1] DER Gateway		x							
[SYS-DER-2] DER Switche		x							
[SYS-Pros-1] External Smart Meter Gateway								x	
[SYS-Pros-2] Pros Switche								x	
[IND-DER-1 Device Energy Management		x							
[IND-DER-2] DER Equipment 1	x								
[IND-Pros-1] Internal Smart Meter Gateway								x	
[IND- Pros -2] DER Equipment 2									x

Tabelle 3: Scope 06 VPP - Zuordnung Systeme zu Infrastruktur

Zuordnung der Systeme zu den Netzen / Kommunikationsverbindungen

(Systeme werden den Netzen / Kommunikationsverbindungen zugeordnet, in denen sie sich befinden bzw. zu denen sie Schnittstellen haben.)

	[NET-1-AV1] External SMGW zum SM	[NET-1/6-AV2] External SMGW zur Leitwarte	[NET-6-AV1] Leitwarte zum EDMS	[NET-6-AV2] Leitwarte zum DMS	[NET-6-AV3] Leitwarte zum SM	[NET-6-AV4] Leitwarte zum Market UI 1	[NET-2-AV1] H&B Integration Bus und CEM UI	[NET-7-AV1] External SMGW und MID Meter 2	[NET-7-AV2] Internal SMGW und CEM	[NET-Pros-2] Home & Building Integration Bus	[NET-DER-3] DER Integration Bus	[NET-CC-4] Intra-center Integration Bus	[NET-5] Operator Backhaul Network	[NET-Pros-7] Direct Wire Connection
[SYS-CC-1] DER SCADA System												x		
[SYS-CC-2] Energy Management System												x		
[SYS-CC-3] Forecasting System for the Generation of Renewable Energy Units												x		
[SYS-CC-4] EMS User Interface												x		
[SYS-CC-5] Domain Controller Leitwarte												x		
[SYS-CC-6] Arbeitsplatzrechner Leitwarte												x		
[SYS-CC-7] Switche Leitwarte												x		
[SYS-CC-8] Firewall Leitwarte		x	x	x	x	x						x	x	
[SYS-DER-1] DER Gateway											x		x	
[SYS-DER-2] DER Switche											x			
[SYS-Pros-1] External Smart Meter Gateway	x	x						x						x
[SYS-Pros-2] Pros Switche							x			x				
[IND-DER-1] Device Energy Management											x			
[IND-DER-2] DER Equipment 1											x			
[IND-Pros-1] Internal Smart Meter Gateway									x					x
[IND- Pros -2] DER Equipment 2										x				

Tabelle 4: Zuordnung Systeme zu Netzen/Kommunikationsverbindungen

5 Schutzbedarfsfeststellung

Die Schutzbedarfsfeststellung für ein virtuelles Kraftwerk erfolgt nach BSI-Standard 200-2 (Standard-Absicherung, Kapitel 8.2) in mehreren Schritten. Sie hat immer individuell zu erfolgen. Dieses Profil enthält einen sinnvollen Vorschlag, an dem sich die individuelle Schutzbedarfsfeststellung orientieren kann.

5.1 Schutzbedarfskategorien

Schadensszenarien
Für die Einschätzung der Schadensauswirkungen werden die Schadensszenarien des BSI 200-2 mit einigen Ergänzungen übernommen:

1. Verstoß gegen Gesetze / Vorschriften / Verträge
2. Beeinträchtigung des informationellen Selbstbestimmungsrechtes
3. Beeinträchtigung der persönlichen Unversehrtheit mit Berücksichtigung des betroffenen Bevölkerungsanteils
4. Beeinträchtigung der Aufgabenerfüllung einschließlich Versorgung und Energiefluss
5. Negative Innen- und Außenwirkung
6. Finanzielle Auswirkungen
7. Anzahl Betroffener und Auswirkungen auf weitere Infrastrukturen

Schutzbedarfskategorien

Schadensszenario	Schutzbedarfskategorie „normal“
1. Verstoß gegen Gesetze / Vorschriften / Verträge	• Verstöße gegen Gesetze / Vorschriften / allgemeine Richtlinien oder Ordnungswidrigkeiten ohne strafrechtliche Konsequenzen. • Geringfügige Vertragsverletzungen mit maximal geringen Konventionalstrafen. • Interne Vereinbarungen (z. B. über Verfügbarkeit) können nicht eingehalten werden.

Schadensszenario	Schutzbedarfskategorie „normal“
2. Beeinträchtigung des informationellen Selbstbestimmungsrechtes	• Es handelt sich um personenbezogene Daten, durch deren Verarbeitung bzw. Missbrauch der Betroffene in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen beeinträchtigt sein kann. • Es sind keine besonderen personenbezogenen Daten betroffen. • Eine Beeinträchtigung des informationellen Selbstbestimmungsrechtes würde durch den Betroffenen als tolerabel eingeschätzt werden. • Personenbezogene Daten würden nicht einen eng begrenzten Bereich verlassen.
3. Beeinträchtigung der persönlichen Unversehrtheit mit Berücksichtigung des betroffenen Bevölkerungsanteils	• Eine Beeinträchtigung der persönlichen Unversehrtheit erscheint nicht möglich oder unwahrscheinlich. • Für einen begrenzten Personenkreis können geringfügige Beeinträchtigungen auftreten.
4. Beeinträchtigung der Aufgabenerfüllung einschließlich Versorgung und Energiefluss	• Die Beeinträchtigung würde von den Betroffenen als tolerabel eingeschätzt werden. • Die maximal tolerierbare Ausfallzeit ist größer als 24 Stunden.
5. Negative Innen- und Außenwirkung	• Eine geringe oder nur interne Ansehens- oder Vertrauensbeeinträchtigung ist zu erwarten. • Negative Publicity in begrenztem Umfang für kurze Dauer in Bezug auf angebotene Leistungen.
6. Finanzielle Auswirkungen	• Der finanzielle Schaden bleibt für die Organisation tolerabel und gefährdet den Betrieb nicht grundsätzlich. • Der Schaden liegt unter x % (z. B. 0,5 %) des Jahresumsatzes der betroffenen Organisation.
7. Anzahl Betroffener und Auswirkungen auf weitere Infrastrukturen	• Es sind weniger als 500 000 Personen betroffen (fällt nicht unter BSI-KritisV). • Weitere Infrastrukturen (z. B. vor- und nachgelagerte Netzbetreiber, Wasserversorgung) werden bei der Erfüllung ihrer Kernaufgaben nicht oder nur geringfügig behindert.

Schadens-Szenario	In die Schutzbedarfskategorie „hoch“ gehört:
1. Verstoß gegen Gesetze / Vorschriften / Verträge	• Verstöße gegen Gesetze / Vorschriften mit erheblichen bzw. strafrechtlichen Konsequenzen. • Vertragsverletzungen mit hohen Konventionalstrafen. • Nationale Vereinbarungen (z. B. über Verfügbarkeit) können nicht eingehalten werden

Schadens-Szenario	In die Schutzbedarfskategorie „hoch“ gehört:
2. Beeinträchtigung des informationellen Selbstbestimmungsrechtes	• Es handelt sich um personenbezogene Daten, durch deren Verarbeitung bzw. Missbrauch der Betroffene in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen erheblich beeinträchtigt werden kann. • Es wären besondere personenbezogene Daten betroffen. • Eine Beeinträchtigung des informationellen Selbstbestimmungsrechtes würde durch den Betroffenen als nicht tolerabel eingeschätzt werden. • Personenbezogene Daten würden einen eng begrenzten Bereich verlassen.
3. Beeinträchtigung der persönlichen Unversehrtheit mit Berücksichtigung des betroffenen Bevölkerungsanteils	• Eine Beeinträchtigung der persönlichen Unversehrtheit kann nicht mit Bestimmtheit ausgeschlossen werden bzw. ist möglich. • Für einen großen Personenkreis können mittelschwere Beeinträchtigungen auftreten.
4. Beeinträchtigung der Aufgabenerfüllung einschließlich Versorgung und Energiefluss	• Die Beeinträchtigung würde von einzelnen Betroffenen als nicht tolerabel eingeschätzt werden. • Die Erfüllung der Kernaufgaben ist beeinträchtigt, wichtige Bereiche sind gelähmt. • Die maximal tolerierbare Ausfallzeit liegt zwischen einer und 24 Stunden. • Der Betrieb wäre stark eingeschränkt.
5. Negative Innen- und Außenwirkung	• Eine erhebliche bzw. breite Ansehens- oder Vertrauensbeeinträchtigung ist zu erwarten. • Weitreichende negative Publicity von langer Dauer in Bezug auf angebotene Leistungen.
6. Finanzielle Auswirkungen	• Der finanzielle Schaden ist für die Organisation beträchtlich, jedoch nicht existenzbedrohend. • Der Schaden liegt zwischen x und y % (z. B. zwischen 0,5 und 10%) des Jahresumsatzes.
7. Anzahl Betroffener und Auswirkungen auf weitere Infrastrukturen	• Es sind mindestens 500 000 Personen betroffen (fällt unter BSI-KritisV). • Weitere Infrastrukturen (z. B. vor- und nachgelagerte Netzbetreiber, Wasserversorgung) würden bei der Erfüllung ihrer Kernaufgaben stark eingeschränkt.

Schadens-Szenario	In die Schutzbedarfskategorie „sehr hoch“ gehört:
1. Verstoß gegen Gesetze / Vorschriften / Verträge	• Fundamentale Verstöße gegen Gesetze / Vorschriften mit Freiheitsstrafen. • Vertragsverletzungen, deren Haftungsschäden ruinös sind. • Nationale und internationale Vereinbarungen (z. B. über Verfügbarkeit) können nicht eingehalten werden
2. Beeinträchtigung des informationellen Selbstbestimmungsrechtes	• Es handelt sich um personenbezogene Daten, durch deren Verarbeitung bzw. Missbrauch eine Gefahr für Leib und Leben oder die persönliche Freiheit des Betroffenen gegeben ist. • Persönlich, gesellschaftlich oder wirtschaftlich ruinöse Folgen für die Betroffenen.
3. Beeinträchtigung der persönlichen Unversehrtheit mit Berücksichtigung des betroffenen Bevölkerungsanteils	• Gravierende Beeinträchtigungen der persönlichen Unversehrtheit sind möglich. • Gefahr für Leib und Leben • Für einen großen Personenkreis können schwere Beeinträchtigungen auftreten.
4. Beeinträchtigung der Aufgabenerfüllung einschließlich Versorgung und Energiefluss	• Die Beeinträchtigung würde von allen Betroffenen als nicht tolerabel eingeschätzt werden. • Die Erfüllung der Kernaufgaben ist nicht mehr möglich. • Die maximal tolerierbare Ausfallzeit ist kleiner als eine Stunde.
5. Negative Innen- und Außenwirkung	• Eine landesweite Ansehens- oder Vertrauensbeeinträchtigung, evtl. existenzgefährdender Art, ist denkbar.
6. Finanzielle Auswirkungen	• Der finanzielle Schaden ist für die Organisation existenzbedrohend. • Der Schaden liegt über y % (z.B. 10 %) des Jahresumsatzes der betroffenen Organisation.
7. Anzahl Betroffener und Auswirkungen auf weitere Infrastrukturen	• Es sind mindestens 500 000 Personen betroffen (fällt unter BSI-KritisV). • Weitere Infrastrukturen (z. B. vor- und nachgelagerte Netzbetreiber, Wasserversorgung) werden an der Erfüllung ihrer Kernaufgaben so stark gehindert, dass sie sie nicht mehr erfüllen können.

5.2 Vorschläge für Schutzbedarfe

5.2.1 Geschäftsprozesse

Geschäftsprozess / Anwendung	Schutzbedarf	Begründung

[PROZ-1] Standardbetrieb (Planung und Steuerung) des virtuellen Kraftwerks Im Folgenden werden dabei die beiden Fälle „[PROZ-4] Bereitstellung von Regelenergie“ und „[PROZ-5] Bereitstellung von Energie und Handel an der Strombörse“ unterschieden.	Vertraulichkeit: normal	Mess- und Steuerdaten haben nur eine zeitlich begrenzte Gültigkeit. Ihre Offenlegung führt zu keinem unmittelbarem Schaden.
	Integrität: hoch	Gezielte Manipulationen, die nicht kurzfristig erkannt und behoben werden können, können zu kritischen Netzsituationen führen.
	Verfügbarkeit: normal	Das virtuelle Kraftwerk kann im Standardbetrieb in bestimmten Grenzen auch ohne Überwachung und aktive Eingriffe funktionsfähig sein. Darüber hinaus existieren Redundanzen und Notfallmechanismen bei den Energieversorgern.
	Authentizität: hoch	Nichtautorisierte, die eine andere Identität vortäuschen, könnten gezielte Manipulationen durchführen, die nicht kurzfristig erkannt und behoben werden können, was zu kritischen Netzsituationen führen kann.
[PROZ-2] Netzüberlast und Abschaltung der DER Energieerzeugung	Vertraulichkeit: normal	Mess- und Steuerdaten haben nur eine zeitlich begrenzte Gültigkeit. Ihre Offenlegung führt zu keinem unmittelbarem Schaden.
	Integrität: hoch	Gezielte Manipulationen, die nicht kurzfristig erkannt und behoben werden können, können zu kritischen Netzsituationen führen bzw. bei einer aus anderen Gründen vorliegenden kritischen Netzsituation diese verschärfen.
	Verfügbarkeit: hoch	In kritischen Netzsituation ist es wichtig die Lagedaten zu kennen und schnell reagieren zu können, um mögliche Schäden zu minimieren.
	Authentizität: hoch	Nichtautorisierte, die eine andere Identität vortäuschen, könnten gezielte Manipulationen durchführen, die nicht kurzfristig erkannt und behoben werden können, was in kritischen Netzsituationen zu einer Verschärfung der Lage führen kann.
[PROZ-3] Abrechnung von Verbrauchs- / Erzeugerdaten	Vertraulichkeit: hoch	Es sind personenbezogene Daten in großem Umfang betroffen. Es muss damit gerechnet werden, dass eine Offenlegung von Verbrauchsdaten von einigen der Betroffenen als nicht tolerabel eingeschätzt werden würde.
	Integrität: normal	Voraussichtlich könnten Fehler / Manipulationen soweit behoben werden, dass finanzielle Schäden begrenzt bleiben und kein schwerwiegender Verstoß gegen Gesetze und Verträge vorliegt und der Ansehensverlust begrenzt bleibt. **Diese Einschätzung ist bei der Anwendung des Grundschutzprofils für den konkreten Informationsverbund zu überprüfen, denkbar ist, dass hier auch ein hoher Schutzbedarf vorliegen kann aufgrund von personenbezogenen Daten.**
	Verfügbarkeit: normal	Voraussichtlich könnte der Ausfall der Abrechnung von Verbrauchs- / Erzeugerdaten durch Rückfallebenen und Erfahrungswerten soweit abgefedert werden, dass finanzielle Schäden begrenzt bleiben und kein schwerwiegender Verstoß gegen Gesetze und Verträge vorliegt und der Ansehensverlust begrenzt bleibt.
	Authentizität: normal	Voraussichtlich würden vorgetäuschte Abrechnungen von Verbrauchs- / Erzeugerdaten erkannt wer-

		den und der Schaden könnte soweit behoben werden, dass er finanziell begrenzt bleibt und kein schwerwiegender Verstoß gegen Gesetze und Verträge vorliegt und der Ansehensverlust begrenzt bleibt.
[PROZ-4] Bereitstellung von Regelenergie	Vertraulichkeit: normal	Mess- und Steuerdaten haben nur eine zeitlich begrenzte Gültigkeit. Ihre Offenlegung führt zu keinem unmittelbarem Schaden.
	Integrität: hoch	Gezielte Manipulationen, die nicht kurzfristig erkannt und behoben werden können, können zu kritischen Netzsituationen führen. Zudem gibt es erhöhte Anforderungen in Bezug auf Regelenergie.
	Verfügbarkeit: hoch	Das virtuelle Kraftwerk kann im Standardbetrieb in bestimmten Grenzen auch ohne Überwachung und aktive Eingriffe funktionsfähig sein. Darüber hinaus existieren Redundanzen und Notfallmechanismen bei den Energieversorgern. Allerdings gibt es erhöhte Anforderungen in Bezug auf Regelenergie.
	Authentizität: hoch	Nichtautorisierte, die eine andere Identität vortäuschen, könnten gezielte Manipulationen durchführen, die nicht kurzfristig erkannt und behoben werden können, was zu kritischen Netzsituationen führen kann. Zudem gibt es erhöhte Anforderungen in Bezug auf Regelenergie.
[PROZ-5] Bereitstellung von Energie und Handel an der Strombörse	Vertraulichkeit: normal	Mess- und Steuerdaten haben nur eine zeitlich begrenzte Gültigkeit. Ihre Offenlegung führt zu keinem unmittelbarem Schaden.
	Integrität: hoch	Gezielte Manipulationen, die nicht kurzfristig erkannt und behoben werden können, können zu kritischen Netzsituationen führen.
	Verfügbarkeit: normal	Das virtuelle Kraftwerk kann im Standardbetrieb in bestimmten Grenzen auch ohne Überwachung und aktive Eingriffe funktionsfähig sein. Darüber hinaus existieren Redundanzen und Notfallmechanismen bei den Energieversorgern.
	Authentizität: hoch	Nichtautorisierte, die eine andere Identität vortäuschen, könnten gezielte Manipulationen durchführen, die nicht kurzfristig erkannt und behoben werden können, was zu kritischen Netzsituationen führen kann.

5.2.2 Anwendungen

Geschäftsprozess / Anwendung	Schutzbedarf	Begründung
[ANW-1] Energie Managementsystem	Vertraulichkeit: hoch	Die Anwendung dient nur dem Geschäftsprozess [PROZ-3] Abrechnung von Verbrauchs- / Erzeugerdaten und übernimmt dessen Schutzbedarf: Es sind personenbezogene Daten in großem Umfang betroffen. Es muss damit gerechnet werden, dass eine Offenlegung von Verbrauchsdaten von einigen der Betroffenen als nicht tolerabel eingeschätzt werden würde.
	Integrität: normal	Die Anwendung dient nur dem Geschäftsprozess [PROZ-3] Abrechnung von Verbrauchs- / Erzeuger-

		daten und übernimmt dessen Schutzbedarf: Voraussichtlich könnten Fehler / Manipulationen soweit behoben werden, dass finanzielle Schäden begrenzt bleiben und kein schwerwiegender Verstoß gegen Gesetze und Verträge vorliegt und der Ansehensverlust begrenzt bleibt. **Diese Einschätzung ist bei der Anwendung des Grundschutzprofils für den konkreten Informationsverbund zu überprüfen, denkbar ist, dass hier auch ein hoher Schutzbedarf vorliegen kann aufgrund von personenbezogenen Daten.**
	Verfügbarkeit: normal	Die Anwendung dient nur dem Geschäftsprozess [PROZ-3] Abrechnung von Verbrauchs- / Erzeugerdaten und übernimmt dessen Schutzbedarf: Voraussichtlich könnte der Ausfall der Abrechnung von Verbrauchs- / Erzeugerdaten durch Rückfallebenen und Erfahrungswerte soweit abgefedert werden, dass finanzielle Schäden begrenzt bleiben und kein schwerwiegender Verstoß gegen Gesetze und Verträge vorliegt und der Ansehensverlust begrenzt bleibt.
	Authentizität: normal	Die Anwendung dient nur dem Geschäftsprozess [PROZ-3] Abrechnung von Verbrauchs- / Erzeugerdaten und übernimmt dessen Schutzbedarf: Voraussichtlich würden vorgetäuschte Abrechnungen von Verbrauchs- / Erzeugerdaten erkannt werden und der Schaden könnte soweit behoben werden, dass er finanziell begrenzt bleibt und kein schwerwiegender Verstoß gegen Gesetze und Verträge vorliegt und der Ansehensverlust begrenzt bleibt.
[ANW-2] Vorhersagesystem	Vertraulichkeit: normal	Die Anwendung dient den Geschäftsprozessen [PROZ-1] Standardbetrieb und [PROZ-2] Netzüberlast und Abschaltung. Vorhersagedaten haben nur eine zeitlich begrenzte Gültigkeit. Ihre Offenlegung führt zu keinem unmittelbarem Schaden.
	Integrität: hoch	Die Anwendung dient den Geschäftsprozessen [PROZ-1] Standardbetrieb und [PROZ-2] Netzüberlast und Abschaltung. Gezielte Manipulationen, die nicht kurzfristig erkannt und behoben werden können, können zu kritischen Netzsituationen führen bzw. bei einer aus anderen Gründen vorliegenden kritischen Netzsituation diese verschärfen.
	Verfügbarkeit: normal	Die Anwendung dient den Geschäftsprozessen [PROZ-1] Standardbetrieb und [PROZ-2] Netzüberlast und Abschaltung.
	Authentizität: normal	Die Anwendung dient den Geschäftsprozessen [PROZ-1] Standardbetrieb und [PROZ-2] Netzüberlast und Abschaltung.
[ANW-3] Kontroll- und Steuerungssystem	Vertraulichkeit: normal	Die Anwendung dient den Geschäftsprozessen [PROZ-1] Standardbetrieb und [PROZ-2] Netzüberlast und Abschaltung, sowie [PROZ-4] Bereitstellung von Regelenergie und [PROZ-5] Bereitstellung von Energie und Handel an der Strombörse. Kontroll- und Steuerdaten haben nur eine zeitlich begrenzte Gültigkeit. Ihre Offenlegung führt zu keinem unmittelbarem Schaden.

	Integrität: hoch	Die Anwendung dient den Geschäftsprozessen [PROZ-1] Standardbetrieb und [PROZ-2] Netzüberlast und Abschaltung, sowie [PROZ-4] Bereitstellung von Regelenergie und [PROZ-5] Bereitstellung von Energie und Handel an der Strombörse. Gezielte Manipulationen, die nicht kurzfristig erkannt und behoben werden können, können zu kritischen Netzsituationen führen bzw. bei einer aus anderen Gründen vorliegenden kritischen Netzsituation diese verschärfen.
	Verfügbarkeit: hoch	Die Anwendung dient den Geschäftsprozessen [PROZ-1] Standardbetrieb und [PROZ-2] Netzüberlast und Abschaltung, sowie [PROZ-4] Bereitstellung von Regelenergie und [PROZ-5] Bereitstellung von Energie und Handel an der Strombörse. Bei Nichtverfügbarkeit können kritische Situationen zu spät erkannt werden oder bei erkannten Störungen kann nicht rechtzeitig reagiert werden.
	Authentizität: hoch	Die Anwendung dient den Geschäftsprozessen [PROZ-1] Standardbetrieb und [PROZ-2] Netzüberlast und Abschaltung, sowie [PROZ-4] Bereitstellung von Regelenergie und [PROZ-5] Bereitstellung von Energie und Handel an der Strombörse. Nicht authentische Informationen sind ähnlich kritisch wie nicht integre.
[ANW-4] Netzdienste, Benutzer- und Ressourcenverwaltung	Vertraulichkeit: normal	Credentials sind geschützt. Die Offenlegung anderer Daten ist unkritisch.
	Integrität: normal	Gezielte, nicht schnell erkennbare Verletzungen der Integrität erscheinen nur schwer möglich.
	Verfügbarkeit: hoch	Die Funktionen sind grundlegend für den IT-Betrieb.
	Authentizität: normal	Gezielte, nicht schnell erkennbare Verletzungen der Authentizität erscheinen nur schwer möglich.
[ANW-5] Büroanwendungen	Vertraulichkeit: normal	Die Bewertung mit „normal“ geht davon aus, das mit den Büroanwendungen keine besonderen personenbezogenen Daten bearbeitet werden.
	Integrität: normal	Integritätsverletzungen hätten keine Auswirkungen auf die Energieversorgung.
	Verfügbarkeit: normal	Ausfälle hätten keine Auswirkungen auf die Energieversorgung.
	Authentizität: normal	Authentizitätsverletzungen hätten keine Auswirkungen auf die Energieversorgung.

5.2.3 IT-Systeme, ICS-Systeme und sonstige Geräte

System / Gerät	Schutzbedarf	Begründung
[SYS-CC-1] DER SCADA System	Vertraulichkeit: normal	Maximumprinzip, geerbt von [ANW-3] Kontroll- und Steuerungssystem
	Integrität: hoch	Maximumprinzip, geerbt von [ANW-3] Kontroll- und Steuerungssystem
	Verfügbarkeit: hoch	Maximumprinzip, geerbt von [ANW-3] Kontroll- und Steuerungssystem
	Authentizität: hoch	Maximumprinzip, geerbt von [ANW-3] Kontroll- und Steuerungssystem

[SYS-CC-2] Energy Management System	Vertraulichkeit: hoch	Maximumprinzip, geerbt von [ANW-1] Energie Managementsystem
	Integrität: normal	Maximumprinzip, geerbt von [ANW-1] Energie Managementsystem
	Verfügbarkeit: normal	Maximumprinzip, geerbt von [ANW-1] Energie Managementsystem
	Authentizität: normal	Maximumprinzip, geerbt von [ANW-1] Energie Managementsystem
[SYS-CC-3] Forecasting System for the Generation of Renewable Energy Units	Vertraulichkeit: normal	Maximumprinzip, geerbt von [ANW-2] Vorhersagesystem
	Integrität: hoch	Maximumprinzip, geerbt von [ANW-2] Vorhersagesystem
	Verfügbarkeit: normal	Maximumprinzip, geerbt von [ANW-2] Vorhersagesystem
	Authentizität: normal	Maximumprinzip, geerbt von [ANW-2] Vorhersagesystem
[SYS-CC-4] EMS User Interface	Vertraulichkeit: hoch	Maximumprinzip, geerbt von [ANW-1] Energie Managementsystem
	Integrität: normal	Maximumprinzip, geerbt von [ANW-1] Energie Managementsystem
	Verfügbarkeit: normal	Maximumprinzip, geerbt von [ANW-1] Energie Managementsystem
	Authentizität: normal	Maximumprinzip, geerbt von [ANW-1] Energie Managementsystem
[SYS-CC-5] Domain Controller Leitwarte	Vertraulichkeit: normal	Maximumprinzip, geerbt von [ANW-4] Netzdienste, Benutzer- und Ressourcenverwaltung
	Integrität: normal	Maximumprinzip, geerbt von [ANW-4] Netzdienste, Benutzer- und Ressourcenverwaltung
	Verfügbarkeit: hoch	Maximumprinzip, geerbt von [ANW-4] Netzdienste, Benutzer- und Ressourcenverwaltung
	Authentizität: normal	Maximumprinzip, geerbt von [ANW-4] Netzdienste, Benutzer- und Ressourcenverwaltung
[SYS-CC-6] Arbeitsplatzrechner Leitwarte	Vertraulichkeit: normal	Maximumprinzip, geerbt von [ANW-5] Büroanwendungen
	Integrität: normal	Maximumprinzip, geerbt von [ANW-5] Büroanwendungen
	Verfügbarkeit: normal	Maximumprinzip, geerbt von [ANW-5] Büroanwendungen
	Authentizität: normal	Maximumprinzip, geerbt von [ANW-5] Büroanwendungen
[SYS-CC-7] Switche Leitwarte	Vertraulichkeit: normal	Maximumprinzip, geerbt von [ANW-4] Netzdienste, Benutzer- und Ressourcenverwaltung
	Integrität: normal	Maximumprinzip, geerbt von [ANW-4] Netzdienste, Benutzer- und Ressourcenverwaltung
	Verfügbarkeit: normal	Verteileffekt, es sind Redundanzen vorhanden.
	Authentizität: normal	Maximumprinzip, geerbt von [ANW-4] Netzdienste, Benutzer- und Ressourcenverwaltung
[SYS-CC-8] Firewall Leitwarte	Vertraulichkeit: normal	Maximumprinzip, geerbt von [ANW-4] Netzdienste, Benutzer- und Ressourcenverwaltung
	Integrität: hoch	Kumulationseffekt, zentrale Sicherheitsinfrastruktur
	Verfügbarkeit: hoch	Maximumprinzip, geerbt von [ANW-4] Netzdienste, Benutzer- und Ressourcenverwaltung
	Authentizität: hoch	Kumulationseffekt, zentrale Sicherheitsinfrastruktur

[SYS-DER-1] DER Gateway	Vertraulichkeit: normal	Maximumprinzip, geerbt von [ANW-3] Kontroll- und Steuerungssystem
	Integrität: hoch	Maximumprinzip, geerbt von [ANW-3] Kontroll- und Steuerungssystem
	Verfügbarkeit: hoch	Maximumprinzip, geerbt von [ANW-3] Kontroll- und Steuerungssystem
	Authentizität: hoch	Maximumprinzip, geerbt von [ANW-3] Kontroll- und Steuerungssystem
[SYS-DER-2] DER Switche	Vertraulichkeit: normal	Maximumprinzip, geerbt von [ANW-4] Netzdienste, Benutzer- und Ressourcenverwaltung
	Integrität: normal	Maximumprinzip, geerbt von [ANW-4] Netzdienste, Benutzer- und Ressourcenverwaltung
	Verfügbarkeit: normal	Verteileffekt, es sind Redundanzen vorhanden.
	Authentizität: normal	Maximumprinzip, geerbt von [ANW-4] Netzdienste, Benutzer- und Ressourcenverwaltung
[IND-DER-1] Device Energy Management	Vertraulichkeit: normal	Maximumprinzip, geerbt von [ANW-3] Kontroll- und Steuerungssystem
	Integrität: hoch	Maximumprinzip, geerbt von [ANW-3] Kontroll- und Steuerungssystem
	Verfügbarkeit: hoch	Maximumprinzip, geerbt von [ANW-3] Kontroll- und Steuerungssystem
	Authentizität: hoch	Maximumprinzip, geerbt von [ANW-3] Kontroll- und Steuerungssystem
[IND-DER-2] DER Equipment 1	Vertraulichkeit: normal	Maximumprinzip, geerbt von [ANW-3] Kontroll- und Steuerungssystem
	Integrität: normal	Verteileffekt: Integritätsverlust bezüglich einzelner Anlagen führt nur zu begrenztem Schaden.
	Verfügbarkeit: normal	Verteileffekt: Ausfall einzelner Anlagen führt nur zu begrenztem Schaden.
	Authentizität: normal	Verteileffekt: Authentizitätsverlust bezüglich einzelner Anlagen führt nur zu begrenztem Schaden.
[IND-Pros-1] Internal Smart Meter Gateway	Vertraulichkeit: hoch	Die Bewertung mit „hoch“ geht davon aus, dass sensible personenbezogene Metering-Daten verarbeitet werden.
	Integrität: hoch	Maximumprinzip, geerbt von [ANW-3] Kontroll- und Steuerungssystem
	Verfügbarkeit: hoch	Maximumprinzip, geerbt von [ANW-3] Kontroll- und Steuerungssystem
	Authentizität: hoch	Maximumprinzip, geerbt von [ANW-3] Kontroll- und Steuerungssystem
[IND-Pros-2] DER Equipment 2	Vertraulichkeit: normal	Maximumprinzip, geerbt von [ANW-3] Kontroll- und Steuerungssystem
	Integrität: normal	Verteileffekt: Integritätsverlust bezüglich einzelner Anlagen führt nur zu begrenztem Schaden.
	Verfügbarkeit: normal	Verteileffekt: Ausfall einzelner Anlagen führt nur zu begrenztem Schaden.
	Authentizität: normal	Verteileffekt: Authentizitätsverlust bezüglich einzelner Anlagen führt nur zu begrenztem Schaden.
[SYS-Pros-1] External Smart Meter Gateway	Vertraulichkeit: hoch	Die Bewertung mit „hoch“ geht davon aus, dass sensible personenbezogene Metering-Daten verarbeitet werden.
	Integrität: hoch	Maximumprinzip, geerbt von [ANW-3] Kontroll- und Steuerungssystem
	Verfügbarkeit: hoch	Maximumprinzip, geerbt von [ANW-3] Kontroll- und Steuerungssystem

	Authentizität: hoch	Maximumprinzip, geerbt von [ANW-3] Kontroll- und Steuerungssystem
[SYS-Pros-2] Pros Switche	Vertraulichkeit: normal	Maximumprinzip, geerbt von [ANW-4] Netzdienste, Benutzer- und Ressourcenverwaltung
	Integrität: normal	Maximumprinzip, geerbt von [ANW-4] Netzdienste, Benutzer- und Ressourcenverwaltung
	Verfügbarkeit: normal	Verteileffekt, es sind Redundanzen vorhanden.
	Authentizität: normal	Maximumprinzip, geerbt von [ANW-4] Netzdienste, Benutzer- und Ressourcenverwaltung

5.2.4 Infrastruktur

Infrastruktur	**Schutzbedarf**	**Begründung**
[INF-DER-1] Betriebsgelände DER-Anlage (enthält DER Equipment 1, z. B. Photovoltaik)	Vertraulichkeit: normal	Maximumprinzip
	Integrität: normal	Maximumprinzip
	Verfügbarkeit: normal	Maximumprinzip
	Authentizität: normal	Maximumprinzip
[INF-DER-2] Betriebsgebäude DER-Anlage (enthält DER Gateway, Device Energy Management)	Vertraulichkeit: normal	Maximumprinzip
	Integrität: hoch	Beherbergte Systeme haben einen hohen SB hinsichtlich Integrität. Das Betriebsgebäude muss daher ausreichend zutrittsgeschützt sein.
	Verfügbarkeit: hoch	Beherbergte Systeme haben einen hohen SB hinsichtlich Verfügbarkeit Das Betriebsgebäude muss daher ausreichend baulich geschützt sein.
	Authentizität: hoch	Beherbergte Systeme haben einen hohen SB hinsichtlich Authentizität. Das Betriebsgebäude muss daher ausreichend zutrittsgeschützt sein.
[INF-CC-1] Unternehmensgebäude (enthält Serverraum, Wartenraum, Büroräume und Technikräume)	Vertraulichkeit: hoch	Maximumprinzip (enthält Serverraum)
	Integrität: hoch	Maximumprinzip (enthält Serverraum)
	Verfügbarkeit: hoch	Maximumprinzip (enthält Serverraum)
	Authentizität: hoch	Maximumprinzip (enthält Serverraum)
[INF-CC-2] Serverraum im Unternehmensgebäude (enthält Energy Management System, Forecasting System for the Generation of Renewable Energy Units, DER SCADA System)	Vertraulichkeit: hoch	Maximumprinzip über die enthaltenen Systeme
	Integrität: hoch	Maximumprinzip über die enthaltenen Systeme
	Verfügbarkeit: hoch	Maximumprinzip über die enthaltenen Systeme
	Authentizität: hoch	Maximumprinzip über die enthaltenen Systeme
[INF-CC-3] Warteraum im Unternehmensgebäude (enthält EMS User Interface)	Vertraulichkeit: hoch	Maximumprinzip über die enthaltenen Systeme
	Integrität: normal	Maximumprinzip über die enthaltenen Systeme
	Verfügbarkeit: normal	Maximumprinzip über die enthaltenen Systeme
	Authentizität:	Maximumprinzip über die enthaltenen Systeme

	normal	
[INF-CC-4] Büroräume im Unternehmensgebäude (enthalten Arbeitsplatzrechner)	Vertraulichkeit: normal	Maximumprinzip über die enthaltenen Systeme
	Integrität: normal	Maximumprinzip über die enthaltenen Systeme
	Verfügbarkeit: normal	Maximumprinzip über die enthaltenen Systeme
	Authentizität: normal	Maximumprinzip über die enthaltenen Systeme
[INF-CC-5] Technikräume im Unternehmensgebäude (enthalten unterstützende Infrastruktur und Versorgungssysteme)	Vertraulichkeit: normal	Es sind keine Daten betroffen.
	Integrität: normal	Es sind keine Daten betroffen.
	Verfügbarkeit: normal	Übliche bauliche Sicherungsmaßnahmen erscheinen ausreichend. Systeme und Anwendungen wären nur indirekt betroffen.
	Authentizität: normal	Es sind keine Daten betroffen.
[INF-Pros-1] Zählerkasten zur Prosumer-DER-Anlage (z. B. im Wohnhaus; enthält External Smart Meter Gateway, Internal Smart Meter Gateway, Customer Energy Management)	Vertraulichkeit: hoch	Maximumprinzip über die enthaltenen Systeme
	Integrität: hoch	Maximumprinzip über die enthaltenen Systeme
	Verfügbarkeit: hoch	Maximumprinzip über die enthaltenen Systeme
	Authentizität: hoch	Maximumprinzip über die enthaltenen Systeme
[INF-Pros-2] Aufstellungsort Prosumer-DER-Anlage (z. B. Dach des Wohnhauses; Aufstellungsort für DER Equipment 2, z. B. Photovoltaik)	Vertraulichkeit: normal	Maximumprinzip über die enthaltenen Systeme
	Integrität: normal	Maximumprinzip über die enthaltenen Systeme
	Verfügbarkeit: normal	Maximumprinzip über die enthaltenen Systeme
	Authentizität: normal	Maximumprinzip über die enthaltenen Systeme

5.2.5 Netze und Kommunikationsverbindungen

Netz / Kommunikationsverbdg.	**SB / Kritikalität**	**Begründung**
[NET-1-AV1] Verbindung External SMGW zum Smart Metering (via AMI Backhaul Network)	Vertraulichkeit: hoch	Es werden personenbezogene Metering-Daten übertragen.
	Integrität: hoch	Eine Integritätsverletzung bei Daten oder Software des verbundenen [SYS-Pros-1] External Smart Meter Gateway kann einen beträchtlichen Schaden hervorrufen.
	Verfügbarkeit: normal	Diese Einstufung anhand den konkreten Zeitanforderungen zu überprüfen.
	Authentizität: normal	Am wichtigsten ist die Korrektheit der Daten; diese ist beim SB der Integrität berücksichtigt.
	Außenverbindung: ☒	Verbindung zum Smart Metering (nicht im IV VK)
	hochschutzbedürftige Informationen dürfen	

	nicht übertragen werden ❑	
[NET-1/6-AV2] Verbindung External SMGW zur Leitwarte (via AMI Backhaul Network und Backbone Network (realisierungsabhängig, z. B. Internet mit Umsetzer dazwischen)	Vertraulichkeit: hoch	Die Bewertung mit „hoch“ geht davon aus, dass sensible personenbezogene Metering-Daten übertragen werden.
	Integrität: hoch	Das angeschlossene [SYS-Pros-1] External Smart Meter Gateway und die übertragenen Daten haben einen hohen Schutzbedarf.
	Verfügbarkeit: normal	Verteileffekt: Der Ausfall der Kommunikation zu einem einzelnen Prosumer über diesen Weg führt noch nicht zu einem größeren Schaden.
	Authentizität: hoch	Das angeschlossene [SYS-Pros-1] External Smart Meter Gateway und die übertragenen Daten haben einen hohen Schutzbedarf.
	Außenverbindung: ☒	Endpunkte gehören zum IV, die dazwischen liegende Kommunikationsinfrastruktur nicht.
	hochschutzbedürftige Informationen dürfen **nicht** übertragen werden ❑	
[NET-6-AV1] Verbindung Leitwarte zum EDMS (via Backbone Network (z. B. Internet))	Vertraulichkeit: normal	Die übertragenen Daten (“DMS approved / supply schedule”) haben durchgängig einen normalen Schutzbedarf.
	Integrität: normal	Die übertragenen Daten (“DMS approved / supply schedule”) haben durchgängig einen normalen Schutzbedarf. Das Firewallsystem der Leitwarte ist gegenüber potentiellen Angriffen über diese Kommunikationsverbindung gehärtet.
	Verfügbarkeit: normal	Die übertragenen Daten (“DMS approved / supply schedule”) haben durchgängig einen normalen Schutzbedarf.
	Authentizität: normal	Die übertragenen Daten (“DMS approved / supply schedule”) haben durchgängig einen normalen Schutzbedarf.
	Außenverbindung: ☒	EDMS liegt außerhalb des IV.
	hochschutzbedürftige Informationen dürfen **nicht** übertragen werden ☒	Das hängt von der realisierten Absicherung der Verbindung ab. Wenn es eine offene oder schwach geschützte Verbindung ist, dann dürften keine hochschutzbedürftigen Informationen übertragen werden.
[NET-6-AV2] Verbindung Leitwarte zum DMS (via Backbone Network (z. B. Internet))	Vertraulichkeit: normal	Die übertragenen Daten (“DMS approved / supply schedule” und „DER supply forecast“) haben durchgängig einen normalen Schutzbedarf.
	Integrität: normal	Die übertragenen Daten (“DMS approved / supply schedule” und „DER supply forecast“) haben durchgängig einen normalen Schutzbedarf. Das Firewallsystem der Leitwarte ist gegenüber potentiellen Angriffen über diese Kommunikationsverbindung gehärtet.
	Verfügbarkeit: normal	Die übertragenen Daten (“DMS approved / supply schedule” und „DER supply forecast“) haben durchgängig einen normalen Schutzbedarf.

	Authentizität: normal	Die übertragenen Daten ("DMS approved / supply schedule" und „DER supply forecast") haben durchgängig einen normalen Schutzbedarf.
	Außenverbindung: ☒	DMS liegt außerhalb des IV.
	hochschutzbedürftige Informationen dürfen **nicht** übertragen werden ☒	Das hängt von der realisierten Absicherung der Verbindung ab. Wenn es eine offene oder schwach geschützte Verbindung ist, dann dürften keine hochschutzbedürftigen Informationen übertragen werden.
[NET-6-AV3] Verbindung Leitwarte zum Smart Metering (via Backbone Network (z. B. Internet))	Vertraulichkeit: hoch	Es werden personenbezogene Daten übertragen („individual metering data").
	Integrität: hoch	Es werden personenbezogene Daten übertragen („individual metering data").
	Verfügbarkeit: normal	Es sind keine zeitkritischen Vorgänge davon abhängig.
	Authentizität: hoch	Es werden personenbezogene Daten übertragen („individual metering data").
	Außenverbindung: ☒	Smart Metering liegt außerhalb des IV.
	hochschutzbedürftige Informationen dürfen **nicht** übertragen werden ❑	
[NET-6-AV4] Verbindung Leitwarte zum Market User Interface 1 (via Backbone Network (z. B. Internet))	Vertraulichkeit: normal	Übertragene Daten sind unkritisch. Es werden keine personenbezogenen Daten übertragen und die Daten sind nach kurzer Dauer nicht mehr aktuell.
	Integrität: normal	Übertragene Daten sind unkritisch. Es sind Mechanismen zur Plausibilitätskontrolle vorhanden.
	Verfügbarkeit: normal	Keine harten zeitlichen Anforderungen bzw. es sind Ausweichmöglichkeiten vorhanden.
	Authentizität: normal	Übertragene Daten sind unkritisch. Es sind Mechanismen zur Plausibilitätskontrolle vorhanden.
	Außenverbindung: ☒	Market User Interface 1 und Kommunikationsinfrastruktur liegen außerhalb des IV.
	hochschutzbedürftige Informationen dürfen **nicht** übertragen werden ☒	Verbindung geht über das Internet, im Falle eines sicheren VPN entfällt diese Kritikalität.
[NET-2-AV1] Verbindung zwischen Home & Building Integration Bus und CEM User Interface (letzteres ist nicht im IV)	Vertraulichkeit: hoch	Es werden personenbezogene Daten übertragen („individual metering data").
	Integrität: hoch	Es werden personenbezogene Daten übertragen („individual metering data").
	Verfügbarkeit: normal	Es sind keine zeitkritischen Vorgänge davon abhängig.
	Authentizität: hoch	Es werden personenbezogene Daten übertragen („individual metering data").
	Außenverbindung: ☒	CEM User Interface liegt außerhalb des IV.
	hochschutzbedürftige Informationen dürfen	

	nicht übertragen werden ❑	
[NET-7-AV1] Verbindung zwischen External SMGW und MID Meter 2 (letzteres ist nicht im IV)	Vertraulichkeit: hoch	Es werden personenbezogene Daten übertragen („individual metering data“).
	Integrität: hoch	Es werden personenbezogene Daten übertragen („individual metering data“).
	Verfügbarkeit: normal	Es sind keine zeitkritischen Vorgänge davon abhängig.
	Authentizität: hoch	Es werden personenbezogene Daten übertragen („individual metering data“).
	Außenverbindung: ☒	MID Meter 2 liegt außerhalb des IV.
	hochschutzbedürftige Informationen dürfen **nicht** übertragen werden ❑	
[NET-7-AV2] Verbindung zwischen Internal SMGW und Customer Energy Management (letzteres ist nicht im IV)	Vertraulichkeit: normal	Es handelt sich um technische Daten / Steuerdaten mit begrenzter Gültigkeit und geringem Wert für einen Angreifer.
	Integrität: hoch	Übertragen werden „Production Setpoint“ und „Switch-off command“. Manipulationen können zu erheblichen Störungen bzw. Ausfällen führen.
	Verfügbarkeit: hoch	Übertragen werden „Production Setpoint“ und „Switch-off command“. Ausfälle der Übertragung dieser Daten können zu erheblichen Störungen bzw. Ausfällen führen.
	Authentizität: hoch	Übertragen werden „Production Setpoint“ und „Switch-off command“. Manipulationen können zu erheblichen Störungen bzw. Ausfällen führen.
	Außenverbindung: ☒	Customer Energy Management liegt außerhalb des IV.
	hochschutzbedürftige Informationen dürfen **nicht** übertragen werden ❑	
[NET-Pros-2] Home & Building Integration Bus	Vertraulichkeit: normal	Die Bewertung hängt davon ab, ob Steuerdaten (hoher SB außer bei der Vertraulichkeit) und Metering Daten (hoher SB bei der Vertraulichkeit) über Home & Building Integration Bus laufen oder über Direktverbindungen.
	Integrität: normal	Die Bewertung hängt davon ab, ob Steuerdaten (hoher SB außer bei der Vertraulichkeit) und Metering Daten (hoher SB bei der Vertraulichkeit) über Home & Building Integration Bus laufen oder über Direktverbindungen.
	Verfügbarkeit: normal	Die Bewertung hängt davon ab, ob Steuerdaten (hoher SB außer bei der Vertraulichkeit) und Metering Daten (hoher SB bei der Vertraulichkeit) über Home & Building Integration Bus laufen oder über Direktverbindungen.

	Authentizität: normal	Die Bewertung hängt davon ab, ob Steuerdaten (hoher SB außer bei der Vertraulichkeit) und Metering Daten (hoher SB bei der Vertraulichkeit) über Home & Building Integration Bus laufen oder über Direktverbindungen.
	Außenverbindung: ❑	Verbindung zu CEM User Interface und Customer Energy Management und MID Meter 2 (nicht im IV VK): Bewertung hängt davon ab wie es dem Home & Building Integration Bus gekoppelt ist
	hochschutzbedürftige Informationen dürfen **nicht** übertragen werden ❑	
[NET-DER-3] DER Integration Bus	Vertraulichkeit: normal	Die übertragenen Kontroll- und Steuerdaten haben nur eine zeitlich begrenzte Gültigkeit. Ihre Offenlegung führt zu keinem unmittelbarem Schaden.
	Integrität: hoch / normal	Übertragen werden „Production Setpoint“ und „Switch-off command“. Manipulationen können zu erheblichen Störungen bzw. Ausfällen führen. Allerdings wäre nur das einzelne lokale System betroffen. Die Einstufung unterliegt dem Verantwortlichen.
	Verfügbarkeit: hoch / normal	Übertragen werden „Production Setpoint“ und „Switch-off command“. Manipulationen können zu erheblichen Störungen bzw. Ausfällen führen. Allerdings wäre nur das einzelne lokale System betroffen. Die Einstufung unterliegt dem Verantwortlichen.
	Authentizität: hoch / normal	Übertragen werden „Production Setpoint“ und „Switch-off command“. Manipulationen können zu erheblichen Störungen bzw. Ausfällen führen. Allerdings wäre nur das einzelne lokale System betroffen. Die Einstufung unterliegt dem Verantwortlichen.
	Außenverbindung: ☒	Verbindung zu MID Meter 1 (nicht im IV VK)
	hochschutzbedürftige Informationen dürfen **nicht** übertragen werden ❑	
[NET-CC-4] Intra-center Integration Bus	Vertraulichkeit: hoch	Maximumprinzip über die angeschlossenen Systeme
	Integrität: hoch	Maximumprinzip über die angeschlossenen Systeme; mehrere angeschlossene Systeme haben einen hohen Schutzbedarf der Integrität für ihre Nutz- und Konfigurationsdaten und ihre Software. Über ein manipuliertes Netz könnten auch Systeme und Anwendungen in der Leitwarte manipuliert werden.
	Verfügbarkeit: hoch	Maximumprinzip über die angeschlossenen Systeme; die Arbeitsfähigkeit der Leitwarte hängt von der Verfügbarkeit des LAN ab.
	Authentizität: hoch	Maximumprinzip über die angeschlossenen Systeme

	Außenverbindung: ❑	LAN, Außenverbindungen ab Firewall
	hochschutzbedürftige Informationen dürfen **nicht** übertragen werden ❑	
[NET-5] Operator Backhaul Network	Vertraulichkeit: normal	Die übertragenen Kontroll- und Steuerdaten haben nur eine zeitlich begrenzte Gültigkeit. Ihre Offenlegung führt zu keinem unmittelbarem Schaden.
	Integrität: hoch	Manipulierte Kontroll- und Steuerdaten können zu einem hohen Schaden führen.
	Verfügbarkeit: hoch	Ein Ausfall der Verbindung hat zur Folge, dass zeitkritische Kontroll- und Steuerdaten nicht übertragen werden können.
	Authentizität: hoch	Durch einen Angreifer eingeschleuste Kontroll- und Steuerdaten können zu einem hohen Schaden führen.
	Außenverbindung: ❑	Logisch vermutlich keine Außenverbindung Verbindet DER Gateway und Leitwarte (Control Center for Virtual Power Plant) über S1 DER SCADA System
	hochschutzbedürftige Informationen dürfen **nicht** übertragen werden ❑	
[NET-Pros-7] Direct Wire Connection	Vertraulichkeit: normal	Es werden personenbezogene Metering-Daten übertragen. Allerdings sind diese auf das jeweilige lokale System bezogen und die Direktverbindungen sind lokal begrenzt.
	Integrität: normal	Übertragen werden „Production Setpoint“ und „Switch-off command“. Manipulationen können grundsätzlich zu erheblichen Störungen bzw. Ausfällen führen. Allerdings wäre nur das einzelne lokale System betroffen und die Direktverbindungen sind lokal begrenzt.
	Verfügbarkeit: normal	Übertragen werden „Production Setpoint“ und „Switch-off command“, welche einen hohen SB bei der Verfügbarkeit besitzen. Allerdings wäre nur das einzelne lokale System betroffen und die Direktverbindungen sind lokal begrenzt.
	Authentizität: normal	Übertragen werden „Production Setpoint“ und „Switch-off command“. Manipulationen können zu erheblichen Störungen bzw. Ausfällen führen. Allerdings wäre nur das einzelne lokale System betroffen und die Direktverbindungen sind lokal begrenzt.
	Außenverbindung: ☒	Mittels direkten Drahtverbindungen sind prosumerseitig Geräte angebunden, die nicht zum IV gehören (MID meter 2, Customer Energy Management).
	hochschutzbedürftige Informationen dürfen **nicht** übertragen werden ❑	

6 Zuordnung der relevanten Bausteine

Basierend auf der Referenzarchitektur mit den relevanten Zielobjekten wird als nächstes der Informationsverbund eines virtuellen Kraftwerks mit Hilfe der im IT-Grundschutz-Kompendium vorhandenen Bausteine nachgebildet zu einem IT-Grundschutz-Modell eines virtuellen Kraftwerks. Grundsätzlich wird empfohlen jeweils alle Basis- und Standardanforderungen der Bausteine zu erfüllen sowie relevante Anforderungen für erhöhten Schutzbedarf sowie ggf. zusätzliche Sicherheitsmaßnahmen zu realisieren.

6.1 Zuordnung der relevanten Prozessbausteine

Baustein	Bezeichnung	Zielobjekte	Begründung / Bemerkung
Prozess-Bausteine:			
ISMS	**Sicherheitsmanagement**		
ISMS.1	Sicherheitsmanagement	Scope 06 VPP	Der Baustein ist einmal für den IV anzuwenden und betrifft das ISMS des verantwortlichen Betreibers des virtuellen Kraftwerks.
ORP	**Organisation und Personal**		
ORP.1	Organisation	Scope 06 VPP	Der Baustein ist einmal für den IV anzuwenden und betrifft die Organisation des verantwortlichen Betreibers des virtuellen Kraftwerks.
ORP.2	Personal	Scope 06 VPP	Der Baustein ist einmal für den IV anzuwenden und betrifft die Regelungen zum Personal des verantwortlichen Betreibers des virtuellen Kraftwerks.
ORP.3	Sensibilisierung und Schulung	Scope 06 VPP	Der Baustein ist einmal für den IV anzuwenden und betrifft Sensibilisierung und Schulung von Mitarbeitern des virtuellen Kraftwerks.
ORP.4	Identitäts- und Berechtigungsmanagement	Scope 06 VPP	Der Baustein ist einmal für den IV anzuwenden und betrifft Identitäts- und Berechtigungsmanagement im virtuellen Kraftwerk.
ORP.5	Compliance Management (Anforderungsmanagement)	Scope 06 VPP	Der Baustein ist einmal für den IV anzuwenden und betrifft den verantwortlichen Betreibers des virtuellen Kraftwerks.
CON	**Konzepte und Vorgehensweisen**		
CON.1	Kryptokonzept	Scope 06 VPP	Der Baustein ist einmal für den IV anzuwenden. Im IV kommen kryptografische Verfahren zum Einsatz.
CON.2	Datenschutz	Scope 06 VPP	Der Baustein ist einmal für den IV anzuwenden. Es werden personenbezogene sowie auf Personen beziehbare Daten verarbeitet.
CON.3	Datensicherungskonzept	Scope 06 VPP	Der Baustein ist einmal für den IV anzuwenden.

Baustein	Bezeichnung	Zielobjekte	Begründung / Bemerkung
CON.4	Auswahl und Einsatz von Standardsoftware	Scope 06 VPP	Der Baustein ist einmal für den IV anzuwenden.
CON.5	Entwicklung und Einsatz von Allgemeinen Anwendungen	Scope 06 VPP	Der Baustein ist einmal für den IV anzuwenden. Es wird spezialisierte Anwendungssoftware eingesetzt.
CON.6	Löschen und Vernichten	Scope 06 VPP	Der Baustein ist einmal für den IV anzuwenden.
CON.7	Informationssicherheit auf Auslandsreisen	- keine Zuordnung -	Nicht relevant, da keine Auslandsreisen absehbar sind.
OPS	**Betrieb**		
OPS 1	**Eigener Betrieb**		
OPS 1.1	**Kern-IT-Betrieb**		
OPS.1.1.2	Ordnungsgemäße IT-Administration	Scope 06 VPP	Der Baustein ist einmal für die IT-Landschaft im IV anzuwenden, welche vom Betreiber des virtuellen Kraftwerks administriert. Im Falle von Outsourcing der IT-Administration, ist er (ggf. mehrfach) für den Outsourcing-Dienstleister anzuwenden.
OPS.1.1.3	Patch- und Änderungsmanagement	Scope 06 VPP	Der Baustein ist einmal für den IV anzuwenden.
OPS.1.1.4	Schutz vor Schadprogrammen	Scope 06 VPP	Dieser Baustein ist so anzuwenden, dass alle IT-Systeme im IV enthalten sind.
OPS.1.1.5	Protokollierung	Scope 06 VPP	Der Baustein ist einmal für den IV anzuwenden.
OPS.1.1.6	Software-Tests und -Freigaben	Scope 06 VPP	Der Baustein ist einmal für den IV anzuwenden.
OPS.1.2	**Weiterführende Aufgaben**		
OPS.1.2.2	Archivierung	- keine Zuordnung - - optional –	Leittechnikprozesse, SCADA-Funktionen und Messwerte können grundsätzlich elektronisch archiviert werden. Ob eine elektronische Langzeitarchivierung im Sinne des Bausteins vorliegt, muss im Einzelfall entschieden werden.
OPS.1.2.3	Informations- und Datenträgeraustausch	- keine Zuordnung -	Datenübertragung mittels Datenträger spielt im IV keine Rolle.
OPS.1.2.4	Telearbeit	- keine Zuordnung -	Telearbeit mittels Datenträger spielt im IV keine Rolle.
OPS 2	**Betrieb von Dritten**		
OPS.2.1	Outsourcing für Kunden	- keine Zuordnung - optional -	Werden im IV Outsourcing-Dienstleistungen in Anspruch genommen, ist dieser Baustein für jede davon anzuwenden.
OPS.2.2	Cloud-Nutzung	- keine Zuordnung - - optional -	Werden im IV Cloud-Dienste genutzt, ist dieser Baustein für jeden davon anzuwenden.
OPS.2.4	Fernwartung	Scope 06 VPP	Der Baustein ist einmal für den IV anzuwenden.
OPS 3	**Betrieb für Dritte**		

Baustein	Bezeichnung	Zielobjekte	Begründung / Bemerkung
OPS.3.1	Outsourcing für Dienstleister	- keine Zuordnung -	Es gibt keinen Dienstleister für Outsourcing im IV.
DER	**Detektion und Reaktion**		
DER.1	Detektion von sicherheitsrelevanten Ereignissen	Scope 06 VPP	Der Baustein ist einmal für den IV anzuwenden.
DER.2	**Security Incident Management**		
DER.2.1	Behandlung von Sicherheitsvorfällen	Scope 06 VPP	Der Baustein ist einmal für den IV anzuwenden.
DER.2.2	Vorsorge für die IT-Forensik	Scope 06 VPP	Der Baustein ist einmal für den IV anzuwenden.
DER.2.3	Bereinigung weitreichender Sicherheitsvorfälle	Scope 06 VPP	Der Baustein wird angewendet im Hinblick auf die Bedrohungslage im Energiesektor durch APT.
DER.3	**Sicherheitsprüfungen**		
DER.3.1	Audits und Revisionen	Scope 06 VPP	Der Baustein ist einmal für den IV anzuwenden.
DER.3.2	Revisionen auf Basis des Leitfadens IS-Revision	- keine Zuordnung -	Es besteht keine Verpflichtung IS-Revisionen auf Basis des Leitfadens IS-Revision durchzuführen.
DER.4	Notfallmanagement	Scope 06 VPP	Der Baustein ist einmal für den IV anzuwenden.

Tabelle 5: Virtuelles Kraftwerk - Modellierung Prozessbausteine

6.2 Zuordnung der relevanten Systembausteine

Baustein	Bezeichnung	Zielobjekte	Begründung / Bemerkung
System-Bausteine:			
APP	**Anwendungen**		
APP.1	**Client-Anwendungen**		
APP.1.1	Office-Produkte	Scope 06 VPP	Der Baustein ist einmal für den IV anzuwenden. Es wird davon ausgegangen, dass in der Leitwarte auch Office-Produkte zum Einsatz kommen.
APP.1.2	Web-Browser	Clients mit Browser in der Leitwarte	Der Baustein wird hier exemplarisch auf „[SYS-CC-6] Arbeitsplatzrechner Leitwarte“ angewendet.
APP.1.4	Mobile Anwendungen (Apps)	- keine Zuordnung – - optional -	Mobile Endgeräte / Apps sind in der Referenzarchitektur nicht vorhanden. Sollten entsprechende Zielobjekte in einem konkreten IV vorhanden sein, sind sie zu modellieren.
APP.2	**Verzeichnisdienst**		
APP.2.1	Allgemeiner Verzeichnisdienst	[ANW-4] Netzdienste, Benutzer- und Ressourcenverwaltung	Zumindest für das LAN der Leitwarte wurde in der Referenzarchitektur davon ausgegangen, dass ein Verzeichnisdienst genutzt wird. Der Baustein wird exemplarisch auf „[ANW-4] Netzdienste, Benutzer-

Baustein	Bezeichnung	Zielobjekte	Begründung / Bemerkung
			und Ressourcenverwaltung“ angewendet. Falls weitere Verzeichnisdienste genutzt werden, ist er entsprechend mehrmals anzuwenden.
APP.2.2	Active Directory	- keine Zuordnung -	Der Verzeichnisdienst ist in der Referenzarchitektur nicht näher spezifiziert. Sollte es ein AD sein, wäre dieser Baustein noch zu modellieren.
APP.2.3	OpenLDAP	- keine Zuordnung -	Der Verzeichnisdienst ist in der Referenzarchitektur nicht näher spezifiziert. Sollte es OpenLDAP sein, wäre dieser Baustein noch zu modellieren.
APP.3	**Netzbasierte Dienste**		
APP.3.1	Webanwendungen	- keine Zuordnung - - optional -	Webanwendungen / Webserver sind in der Referenzarchitektur nicht näher spezifiziert. Es sind auf dem Markt aber Produktlösungen zur Anbindung der dezentralen Anlagen (DER Gateway) verfügbar, die über einen Webserver bedient / parametriert werden. Ebenso ist nicht auszuschließen, dass die Anwendungen in der Leitwarte Webanwendungen / Webserver einsetzen. Falls dies im konkreten Fall zutrifft, ist der Baustein zusätzlich zu modellieren.
APP.3.2	Webserver	- keine Zuordnung - - optional -	Webanwendungen / Webserver sind in der Referenzarchitektur nicht näher spezifiziert. Es sind auf dem Markt aber Produktlösungen zur Anbindung der dezentralen Anlagen (DER Gateway) verfügbar, die über einen Webserver bedient / parametriert werden. Ebenso ist nicht auszuschließen, dass die Anwendungen in der Leitwarte Webanwendungen / Webserver einsetzen. Falls dies im konkreten Fall zutrifft, ist der Baustein zusätzlich zu modellieren.
APP.3.3	Fileserver	- keine Zuordnung - - optional -	Ein Fileserver ist in der Referenzarchitektur nicht spezifiziert. Sollte dies in der konkreten Realisierung der Fall sein, wäre der Baustein zu modellieren.
APP.3.4	Samba	- keine Zuordnung - - optional -	Ein Sambaserver ist in der Referenzarchitektur nicht spezifiziert. Sollte dies in der konkreten Realisierung der Fall sein, wäre der Baustein zu modellieren.
APP.3.6	DNS-Server	- keine Zuordnung - - optional -	Ein DNS Server ist in der Referenzarchitektur nicht spezifiziert. Sollte dies in der konkreten Realisierung der Fall sein, wäre der Baustein zu modellieren.
APP.4	**Business-Anwendungen**		
APP.4.2	SAP-ERP-System	- keine Zuordnung -	Ein SAP-ERP-System ist im IV nicht vorhanden.
APP.4.3	Relationale Datenbanksysteme	[ANW-1] Energie Managementsystem	Der Baustein wird exemplarisch für „[ANW-1] Energie Managementsystem herangezogen.“
APP.4.6	SAP ABAP-Programmierung	- keine Zuordnung -	SAP ABAP-Programmierung ist im IV nicht vorhanden.
APP.5	**E-Mail/ Groupware/ Kommunikation**		
APP.5.1	Allgemeine Groupware	[ANW-5] Büroanwendungen	Es wird angenommen, dass „[ANW-5] Büroanwendungen“ Groupware enthält.

Baustein	Bezeichnung	Zielobjekte	Begründung / Bemerkung
APP.5.2	Microsoft Exchange und Outlook	- keine Zuordnung - - optional -	Sollte die Groupware in „[ANW-5] Büroanwendungen“ Microsoft Exchange und Outlook beinhalten, wäre der Baustein zusätzlich zu modellieren.
SYS	**IT-Systeme**		
SYS.1	**Server**		
SYS.1.1	Allgemeiner Server	[SYS-CC-1] DER SCADA System [SYS-CC-2] Energy Management System [SYS-CC-3] Forecasting System for the Generation of Renewable Energy Units [SYS-CC-5] Domain Controller Leitwarte	Der Baustein wird für alle Server im IV angewendet. In der konkreten Ausgestaltung können noch weitere als die genannten dazukommen.
SYS.1.2	***Windows Server***		
SYS.1.2.1	Windows-Server 2012	- keine Zuordnung - - optional -	Das Betriebssystem der Server ist in der Referenzarchitektur nicht näher spezifiziert. Sollte es Windows-Server 2012 (oder 2016/19) sein, wäre dieser Baustein noch zu modellieren.
SYS.1.3	Server unter UNIX	- keine Zuordnung - - optional -	Das Betriebssystem der Server ist in der Referenzarchitektur nicht näher spezifiziert. Sollte es Linux sein, wäre dieser Baustein noch zu modellieren.
SYS.1.5	Virtualisierung	Scope 06 VPP	Der Baustein wird exemplarisch verwendet, da zunehmend Virtualisierungslösungen zum Einsatz kommen und auch für den IV im konkreten Falle dies nicht ausgeschlossen werden kann.
SYS.1.7	IBM Z-System	- keine Zuordnung -	IBM Z-Systeme sind in der Referenzarchitektur nicht vorhanden. Sie werden in einem IV dieser Art üblicherweise nicht eingesetzt.
SYS.1.8	Speicherlösungen	Scope 06 VPP	Der Baustein wird exemplarisch verwendet, da zunehmend Speicherlösungen zum Einsatz kommen und auch für den IV im konkreten Falle dies nicht ausgeschlossen werden kann.
SYS.2	**Desktop-Systeme**		
SYS.2.1	Allgemeiner Client	[SYS-CC-4] EMS User Interface [SYS-CC-6] Arbeitsplatzrechner Leitwarte	Der Baustein wird für alle Clients im IV angewendet. In der konkreten Ausgestaltung können noch weitere als die genannten dazukommen.
SYS.2.2	***Windows Clients***		
SYS.2.2.2	Clients unter Windows 8.1	- keine Zuordnung - - optional -	Das Betriebssystem der Clients ist in der Referenzarchitektur nicht näher spezifiziert. Sollte es Windows 8.1 sein, wäre dieser Baustein noch zu modellieren.
SYS.2.2.3	Clients unter Windows 10	- keine Zuordnung - - optional -	Das Betriebssystem der Clients ist in der Referenzarchitektur nicht näher spezifiziert. Sollte es Windows 10 sein, wäre dieser Baustein noch zu modellieren.
SYS.2.3	Clients unter Unix	- keine Zuordnung - - optional -	Das Betriebssystem der Clients ist in der Referenzarchitektur nicht näher spezifiziert. Sollte es Linux sein, wäre dieser Baustein noch zu modellieren.

Baustein	Bezeichnung	Zielobjekte	Begründung / Bemerkung
SYS.2.4	Clients unter macOS	- keine Zuordnung - - optional -	Das Betriebssystem der Clients ist in der Referenzarchitektur nicht näher spezifiziert. Sollte es macOS sein, wäre dieser Baustein noch zu modellieren.
SYS.3	**Mobile Devices**		
SYS.3.1	Laptops	- keine Zuordnung - - optional -	Es ist nicht zwingend, dass Laptops eingesetzt werden. Sollte es in der konkreten Realisierung der Fall sein, wäre dieser Baustein noch zu modellieren.
SYS.3.2	***Tablet und Smartphone***		
SYS.3.2.1	Allgemeine Smartphones und Tablets	Scope 06 VPP	Es ist damit zu rechnen, dass in einer konkreten Realisierung auch Smartphones oder einfache Mobiltelefone zum Einsatz kommen, beispielsweise in der Notfallbewältigung.
SYS.3.2.2	Mobile Device Management (MDM)	- keine Zuordnung optional -	Es ist nicht zwingend, dass MDM eingesetzt wird. Sollte es in der konkreten Realisierung der Fall sein, wäre dieser Baustein noch zu modellieren.
SYS.3.2.3	iOS (for Enterprise)	- keine Zuordnung - - optional -	Falls SmartPhones / Handys eingesetzt werden würden, gäbe es mehrere Möglichkeiten für das BS, sollte es iOS sein, wäre der Baustein zusätzlich zu modellieren.
SYS.3.2.4	Android	- keine Zuordnung - - optional -	Falls SmartPhones / Handys eingesetzt werden würden, gäbe es mehrere Möglichkeiten für das BS, sollte es Android sein, wäre der Baustein zusätzlich zu modellieren.
SYS.3.3	Mobiltelefon	Scope 06 VPP	Es ist damit zu rechnen, dass in einer konkreten Realisierung auch Smartphones oder einfache Mobiltelefone zum Einsatz kommen, beispielsweise in der Notfallbewältigung.
SYS.3.4	Mobile Datenträger	Scope 06 VPP	Es ist wahrscheinlich, dass in einer konkreten Realisierung auch mobile Datenträger zum Einsatz kommen.
SYS.4	**Sonstige Systeme**		
SYS.4.1	Drucker, Kopierer und Multifunktionsgeräte	- keine Zuordnung - - optional -	Drucker, Kopierer und Multifunktionsgeräte sind in der Referenzarchitektur nicht erfasst. Sollten sie (vernetzt) vorhanden sein, wäre dieser Baustein noch zu modellieren.
SYS.4.3	Eingebettete Systeme	[IND-DER-1] Device Energy Management [IND-DER-2] DER Equipment 1 [IND-Pros-2] DER Equipment 2	Es ist damit zu rechnen, dass im Bereich der Energieerzeuger und Prosumer Systeme mit eingebetteten Systemen zum Einsatz kommen. Die Modellierung muss im konkreten Fall ggf. erweitert werden.
SYS.4.4	Allgemeines IoT-Gerät	- keine Zuordnung -	nicht relevant
IND	**Industrielle IT**		
IND.1	Betriebs- und Steuerungstechnik	Scope 06 VPP	Der IV enthält Betriebs- und Steuerungstechnik. Vsl. ist der Baustein im konkreten Falle jeweils für einzelne Bereiche mit Betriebstechnik anzuwenden.

Baustein	Bezeichnung	Zielobjekte	Begründung / Bemerkung
IND.2	**ICS-Komponenten**		
IND.2.1	Allgemeine ICS-Komponente	[IND-DER-1] Device Energy Management	Im Bereich der Energieerzeuger und Prosumer kommen ICS-Komponenten zum Einsatz. Die Modellierung erfolgt exemplarisch für das Device Energy Management, sie muss im konkreten Fall vsl. erweitert werden.
IND.2.2	Speicherprogrammierbare Steuerung (SPS)	[IND-DER-1] Device Energy Management	Es ist damit zu rechnen, dass im Bereich der Energieerzeuger und Prosumer Systeme mit SPS zum Einsatz kommen. Die Modellierung erfolgt exemplarisch für das Device Energy Management, sie muss im konkreten Fall vsl. erweitert werden.
IND.2.3	Sensoren und Aktoren	IND-DER-2] DER Equipment 1 [IND-Pros-2] DER Equipment 2	Im Bereich der Energieerzeuger und Prosumer kommen Sensoren und Aktoren zum Einsatz. Die Modellierung erfolgt exemplarisch für DER Equipment, sie muss im konkreten Fall ggf. erweitert werden.
IND.2.4	Maschine	[IND-DER-2] DER Equipment 1 [IND-Pros-2] DER Equipment 2	Der Baustein ist nicht vollständig zutreffend für das DER Equipment. Einzelne Anforderungen können aber sinngemäß zutreffen.
IND.2.7	Safety Instrumented Systems	Scope 06 VPP	Der Baustein wird exemplarisch für das Zusammenwirken des Device Energy Managements mit dem DER Equipment verwendet.
NET	**Netze und Kommunikation**		
NET.1	**Netze**		
NET.1.1	Netzarchitektur und -design	Scope 06 VPP	Der Baustein wird auf das Gesamtnetz des virtuellen Kraftwerks angewendet. Die Anforderungen gelten für das lokale Netz der Leitwarte, die IT-Netze der Erzeuger und Prosumer sowie die genutzten Weitverkehrsverbindungen.
NET.1.2	Netzmanagement	- keine Zuordnung - - optional -	Falls Netzmanagement-Systeme zum Einsatz kommen, wäre der Baustein auf jeden Fall anzuwenden.
NET.2	**Funknetze**		
NET.2.1	WLAN-Betrieb	- keine Zuordnung -	WLAN ist nicht Bestandteil der Referenzarchitektur.
NET.2.2	WLAN-Nutzung	- keine Zuordnung -	WLAN ist nicht Bestandteil der Referenzarchitektur.
NET.3	**Netzkomponenten**		

Baustein	Bezeichnung	Zielobjekte	Begründung / Bemerkung
NET.3.1	Router und Switches	[SYS-CC-7] Switche Leitwarte [SYS-DER-1] DER Gateway [SYS-Pros-1] External Smart Meter Gateway [IND-Pros-1] Internal Smart Meter Gateway	Der Baustein ist auf alle Router und Switche im virtuellen Kraftwerk anzuwenden (hier repräsentiert durch [SYS-CC-7] Switche Leitwarte]). Der Baustein wird auch ersatzweise bzw. sinngemäß für die SMGWs sowie das DER Gateway angewendet.
NET.3.2	Firewall	[SYS-CC-8] Firewall Leitwarte	Der Baustein ist immer anzuwenden, wenn unterschiedlich vertrauenswürdige Netze gekoppelt werden. Er wird exemplarisch auf die Firewall der Leitwarte angewendet.
NET.3.3	VPN	Scope 06 VPP	Bei der Anwendung des Bausteins sind alle Verbindungen die zwischen Standorten des VKw über ein WAN erfolgen, sowie Verbindungen von außen auf Netze / Systeme des VKw einzubeziehen.
NET.4	**Telekommunikation**		
NET.4.1	TK-Anlagen	- keine Zuordnung - - optional -	TK-Anlagen sind in der Referenzarchitektur nicht erfasst. Sollten sie vorhanden sein, wäre dieser Baustein noch zu modellieren.
NET.4.2	VoIP	- keine Zuordnung - - optional -	VoIP ist in der Referenzarchitektur nicht erfasst. Sollten es vorhanden sein, wäre dieser Baustein noch zu modellieren.
NET.4.3	Faxgeräte und Faxserver	- keine Zuordnung - - optional -	Faxgeräte und Faxserver sind in der Referenzarchitektur nicht erfasst. Sollten sie vorhanden sein, wäre dieser Baustein noch zu modellieren.
INF	**Infrastruktur**		
INF.1	Allgemeines Gebäude	[INF-CC-1] Unternehmensgebäude [INF-DER-2] Betriebsgebäude DER-Anlage	Das (Wohn)haus zur Prosumer-DER-Anlage wird nicht modelliert, da davon nur der Zählerkasten zur Prosumer-DER-Anlage, sowie der Aufstellungsort (z. B. Dach) zum IV gehören.
INF.2	Rechenzentrum sowie Serverraum	[INF-CC-2] Serverraum im Unternehmensgebäude	Es ist im konkreten Fall zu entscheiden, ob der Baustein im Sinne eines Rechenzentrums oder im Sinne eines Serverraums anzuwenden ist.
INF.3	Elektrotechnische Verkabelung	[INF-CC-1] Unternehmensgebäude [INF-DER-2] Betriebsgebäude DER-Anlage	Der Baustein ist auf alle relevanten Gebäude im Informationsverbund anzuwenden.

Baustein	Bezeichnung	Zielobjekte	Begründung / Bemerkung
INF.4	IT-Verkabelung	[INF-CC-1] Unternehmensgebäude [INF-DER-2] Betriebsgebäude DER-Anlage	Der Baustein ist auf alle relevanten Gebäude im Informationsverbund anzuwenden.
INF.6	Datenträgerarchiv	- keine Zuordnung - - optional -	Falls im konkreten Fall ein Datenträgerarchiv vorhanden ist, wäre der Bausteine noch zu heranzuziehen.
INF.7	Büroarbeitsplatz	[INF-CC-3] Wartenraum im Unternehmensgebäude [INF-CC-4] Büroräume im Unternehmensgebäude	Für den Wartenraum ist zusätzlich zu prüfen, ob weitere Risikoanalysen erforderlich sind.
INF.8	Häuslicher Arbeitsplatz	- keine Zuordnung -	Nicht vorgesehen.
INF.9	Mobiler Arbeitsplatz	- keine Zuordnung - - optional -	Falls im konkreten Fall der Arbeitsplatz eines mobilen Servicetechnikers zum IV zählen sollte, wäre der Bausteine noch heranzuziehen.
INF.10	Besprechungs-, Veranstaltungs- und Schulungsräume	- keine Zuordnung -	Nicht Teil des VKw.

Tabelle 6: Virtuelles Kraftwerk - Modellierung Systembausteine

Die ausgewählten Systembausteine sind auf die genannten Zielobjekte aus der Referenzarchitektur anzuwenden. Da hinsichtlich der konkreten Implementierungen von Anwendungen, Netzen und Systemen in einem virtuellen Kraftwerk diverse Freiheitsgrade vorliegen, kann hier keine endgültige Bausteinauswahl vorgenommen werden.

7 Sicherheitsanforderungen und umzusetzende Maßnahmen

Die zugeordneten Bausteine enthalten Sicherheitsanforderungen in drei Prioritätsstufen: Basisanforderungen, Standardanforderungen und Anforderungen für erhöhten Schutzbedarf. Grundsätzlich wird empfohlen für die entsprechenden Zielobjekte bzw. dem ganzen Informationsverbund alle Basis- und Standardanforderungen der Bausteine zu erfüllen, sowie die relevante Anforderungen für erhöhten Schutzbedarf. Falls erforderlich, sollte geprüft werden, ob zusätzliche Sicherheitsanforderungen, wie sie etwa in einschlägigen Standards und White Papern vorgeschlagen werden, umzusetzen sind. Dies kann der Fall sein, wenn ein hoher oder sehr hoher Schutzbedarf vorliegt, kein geeigneter Grundschutzbaustein existiert oder besondere Einsatz- oder Randbedingungen vorliegen.

8 Exemplarische Risikoanalyse

8.1 Bewertung der Ausgangslage und Bildung von Risikobereichen

8.1.1 Bewertung der Ausgangslage

Schutzbedarf

Der Informationsverbund des virtuellen Kraftwerks enthält 49 Assets. Davon haben 33 einen hohen Schutzbedarf in mindestens einem der vier Grundwerte. Ein sehr hoher Schutzbedarf wurde nicht identifiziert.
Bezogen auf die Grundwerte sind die Fälle mit hohem Schutzbedarf:

- Vertraulichkeit: 23
- Integrität: 26
- Verfügbarkeit: 18
- Authentizität: 23

Aufgrund des Schutzbedarfes ist es daher erforderlich eine Risikoanalyse durchzuführen.

Modellierbarkeit durch Bausteine

Von den 49 Assets sind 5 Geschäftsprozesse, die nicht modelliert werden (die korrespondierenden Anwendungen werden modelliert). Von den 44 Assets waren

- Vollständig modellierbar: 31
- Teilweise modellierbar: 8
- Deutlich unzureichend modellierbar: 5

Daher ist auch wegen der nicht vollständigen Modellierbarkeit durch Grundschutzbausteine eine Risikoanalyse durchzuführen.

Einsatzszenarien

Die Nutzung von IT-Systemen, Vernetzung und sonstigen technischen Systemen in Wohngebäuden stellt ein besonderes Einsatzszenario dar. Ebenso können aus dem Umstand, dass Erzeugung und Verbrauch von Energie kleinteilig aufgesplittet sind, besondere Randbedingungen erwachsen. Insgesamt spielt das Kriterium *„Einsatzszenarien (Umgebung, Anwendung) die im Rahmen des IT-Grundschutzes nicht vorgesehen sind“* eine weniger wichtige Rolle als die beiden Kriterien *„Schutzbedarf“* und *„Modellierbarkeit*“. Es sollte zusammen mit diesen behandelt werden, und entsprechend werden hierfür keine separaten Risikobereiche gebildet.

8.1.2 Bildung von Risikobereichen aufgrund des Schutzbedarfes

Es sind über alle Asset-Kategorien hinweg Assets mit einem maximalen Schutzbedarf von „normal“ und Assets mit einem maximalen Schutzbedarf von „hoch“ vorhanden, wobei Letzteres überwiegt.
Im Wesentlichen zeigt sich, dass ein hoher Schutzbedarf der Vertraulichkeit (und teilweise auch Integrität und Authentizität) von der Verarbeitung, Übertragung und Speicherung personenbezogener Daten herrührt, während ein hoher Schutzbedarf der Integrität und Authentizität (und teilweise auch Verfügbarkeit) auf der Verarbeitung, Übertragung und Speicherung von Kontroll- und Steuerungsdaten beruht.
Auf oberster Ebene kann für die Schwachstellen-, Bedrohungs- und Risikoanalyse zwischen den beiden Bereichen

„Verlust von Vertraulichkeit (Schwerpunkt), Integrität und Authentizität (besonderer) personenbezogener Daten“
und
„Verlust der Integrität (Schwerpunkt), Authentizität und Verfügbarkeit von Kontroll- und Steuerungsdaten und –funktionen“
unterschieden werden.

8.1.3 Bildung von Risikobereichen aufgrund der Modellierbarkeit

Die drei Assets

- INF-DER-1 Betriebsgelände DER-Anlage (enthält DER Equipment 1, z. B. Photovoltaik)
- INF-Pros-1 Zählerkasten zur Prosumer-DER-Anlage (z. B. im Wohnhaus; enthält External SMGW, Internal SMGW, Customer Energy Management)
- INF-Pros-2 Aufstellungsort Prosumer-DER-Anlage (z. B. Dach des Wohnhauses; Aufstellungsort für DER Equipment 2, z. B. Photovoltaik)

konnten nicht ausreichend durch vorhandene Grundschutzbausteine modelliert werden.

Es handelt sich um Infrastruktur-Assets, bei denen die typischen Gefährdungen in den Bereichen Zutrittskontrolle (bzw. auch im Sinne physischer Zugriffskontrolle beim Zählerkasten) und bauliche / materielle Absicherung liegen. Gemeinsam haben die drei Assets auch, dass sie sich nicht in der Zentrale des virtuellen Kraftwerks befinden, sondern zu dezentralen Erzeugern bzw. Verbrauchern gehören und in einer konkreten Ausprägung in großer Anzahl Teil des virtuellen Kraftwerks sind.
Diese Assets können daher als Risikobereich
„Vorsätzliche Überwindung oder zufällige Schäden (einschließlich höherer Gewalt) bei Infrastruktureinrichtungen der dezentralen Erzeuger bzw. Verbraucher“
zusammengefasst werden.

Die Modellierung von

- SYS-DER-1 DER Gateway und
- SYS-Pros-1 External Smart Meter Gateway

lediglich durch den Baustein NET.3.1 Router und Switches ist ebenfalls unzureichend, da diese IT-Systeme weitere Funktionalität besitzen und insgesamt eine besondere Rolle bei der abgesicherten Kommunikation spielen.
Hinsichtlich der Risikobereiche stellen sie Sonderfälle der im Zusammenhang mit den Schutzbedarfen festgelegten Risikobereiche dar bzw. sind orthogonal dazu. Tabelle 7 verdeutlicht den Zusammenhang.

Risikoanalyse wegen Modellierung / **Risikoanalyse wegen Schutzbedarf**	**SYS-DER-1 DER Gateway**	**SYS-Pros-1 External Smart Meter Gateway**	
„Verlust von Vertraulichkeit (Schwerpunkt), Integrität und Authentizität (besonderer) personenbezogener Daten“		z. B. Abhören pers.bez. Daten im oder bei Übertragung vom / zum SMGW	ggf. weitere (ohne Modellierungsdefizit)

„Verlust der Integrität (Schwerpunkt), Authentizität und Verfügbarkeit von Kontroll- und Steuerungsdaten und –funktionen“	z. B. Eindringen in Steuerungsanlagen über DER Gateway	z. B. Eindringen in Steuerungsanlagen über SMGW	.....

Tabelle 7: Scope 06 „Virtuelles Kraftwerk“ – Zusammenhang Risikobereiche

8.2 Risikoanalysen

8.2.1 Risikobereich „Verlust von Vertraulichkeit (Schwerpunkt), Integrität und Authentizität (besonderer) personenbezogener Daten“

Der Risikobereich kann weiter unterteilt werden, in den Geschäftsprozess „Abrechnung von Verbrauchs- / Erzeugerdaten“ sowie in den Bereich „Smart Metering“.

8.2.1.1 „Abrechnung von Verbrauchs- / Erzeugerdaten“ (1. Risikobereich VPP)

Die an diesem Prozess beteiligten Assets sind in Tabelle 8 aufgelistet.
Bei den Verbrauchs- / Erzeugerdaten handelt es sich um personenbezogene Daten mit einem hohen Schutzbedarf der Vertraulichkeit. Dieser Schutzbedarf überträgt sich auf die beteiligten Assets.

Assets in Scope 06 - Virtuelles Kraftwerk Geschäftsprozess „Abrechnung von Verbrauchs- / Erzeugerdaten“			
Typ	**Bezeichnung**	**ID**	**Baustein(e)**
Geschäftsprozess	Abrechnung von Verbrauchs- / Erzeugerdaten	PROZ-3	–
Anwendung	Energie Managementsystem	ANW-1	APP.4.3
System / Gerät	Energy Management System	SYS-CC-2	SYS.1.1
System / Gerät	EMS User Interface	SYS-CC-4	SYS.2.1
Infrastruktur	Unternehmensgebäude (enthält Serverraum, Warteraum, Büroräume und Technikräume)	INF-CC-1	INF.1 INF.3 INF.4
Infrastruktur	Serverraum im Unternehmensgebäude (enthält Energy Management System, Forecasting System for the Generation of Renewable Energy Units, DER SCADA System)	INF-CC-2	INF.2
Infrastruktur	Warteraum im Unternehmensgebäude (enthält EMS User Interface)	INF-CC-3	INF.7
Netz / Kommunikationsverbindung	Intra-center Integration Bus	NET-CC-4	NET.1.1

Tabelle 8: Assets zum Geschäftsprozess "Abrechnung von Verbrauchs-/Erzeugerdaten"

Den Anforderungen in den IT-Grundschutz-Bausteinen sind jeweils elementare Gefährdungen zugeordnet. „INF.3 Elektrotechnische Verkabelung“ ist im Zusammenhang mit diesem Risikobereich nicht relevant. Bezüglich „INF.4 IT-Verkabelung“ ist lediglich „G 0.15 Abhören“ relevant und wurde in Tabelle 16 ergänzt.
Ansonsten werden die zugeordneten elementaren Gefährdungen in den folgenden Tabellen aufgelistet, ggf. ergänzt, und es werden jeweils Eintrittswahrscheinlichkeit und Schadenshöhe bewertet (die dabei verwendeten Skalen sind von den Verantwortlichen zuvor zu definieren) unter der Voraussetzung, dass die Grundschutzanforderungen erfüllt sind, aber keine zusätzlichen Maßnahmen festgelegt wurden. Daraus wird das jeweilige Risiko abgeleitet. Bei der Bewertung wird berücksichtigt, dass der Schwerpunkt des Risikobereichs beim Verlust der Vertraulichkeit (besonderer) personenbezogener Daten liegt. Elementare Gefährdungen, die in Bezug auf den Risikobereich nicht relevant sind, erhalten keine Bewertung („ - “).

Den Anforderungen im Baustein **APP.4.3 Relationale Datenbanksysteme** (modelliert für Energie Managementsystem ANW-1) sind elementare Gefährdungen zugeordnet, die wie folgt hinsichtlich des Risikobereichs „Verlust von Vertraulichkeit (Schwerpunkt), Integrität und Authentizität (besonderer) personenbezogener Daten“ bewertet werden:

Elementare Gefährdung	Eintrittsw.	Schaden	Risiko	Bemerkung
G 0.14 Ausspähen von Informationen / Spionage	mittel	hoch	mittel	
G 0.15 Abhören	gering	hoch	mittel	
G 0.18 Fehlplanung oder fehlende Anpassung	gering	gering	tragbar	indirekt
G 0.19 Offenlegung schützenswerter Informationen	mittel	hoch	mittel	
G 0.20 Informationen oder Produkte aus unzuverlässiger Quelle	gering	gering	tragbar	indirekt
G 0.21 Manipulation von Hard- oder Software	mittel	hoch	mittel	
G 0.22 Manipulation von Informationen	mittel	gering	tragbar	betrifft nur Integrität
G 0.23 Unbefugtes Eindringen in IT-Systeme	gering	hoch	tragbar	indirekt
G 0.25 Ausfall von Geräten oder Systemen	-	-	-	-
G 0.26 Fehlfunktion von Geräten oder Systemen	mittel	gering	tragbar	indirekt
G 0.27 Ressourcenmangel	gering	gering	tragbar	indirekt
G 0.28 Software-Schwachstellen oder –Fehler		hoch	mittel	
G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen	gering	hoch	tragbar	indirekt
G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen	gering	gering	tragbar	indirekt
G 0.32 Missbrauch von Berechtigungen	mittel	hoch	mittel	Indirekt aber grundlegend
G 0.36 Identitätsdiebstahl	mittel	hoch	mittel	Indirekt aber grundlegend
G 0.37 Abstreiten von Handlungen	gering	gering	tragbar	indirekt
G 0.39 Schadprogramme	mittel	hoch	mittel	indirekt
G 0.40 Verhinderung von Diensten (Denial of Service)	-	-	-	-
G 0.43 Einspielen von Nachrichten	gering	gering	tragbar	betrifft nur Integrität
G 0.45 Datenverlust	-	-	-	-
G 0.46 Integritätsverlust schützenswerter Informationen	gering	gering	tragbar	betrifft nur Integrität

Tabelle 9: Bewertung der elementaren Gefährdung zu APP.4.3 Relationale Datenbanksysteme für den 1. Risikobereich VPP

Den Anforderungen im Baustein **SYS.1.1 Allgemeiner Server** (modelliert für SYS-CC-2 Energy Management System) sind elementare Gefährdungen zugeordnet, die wie folgt hinsichtlich des Risikobereichs „Verlust von Vertraulichkeit (Schwerpunkt), Integrität und Authentizität (besonderer) personenbezogener Daten“ bewertet werden:

Elementare Gefährdung	Eintritt	Schaden	Risiko	Bemerkung
G 0.8 Ausfall oder Störung der Stromversorgung	-	-	-	-
G 0.9 Ausfall oder Störung von Kommunikationsnetzen	mittel	gering	tragbar	indirekt

Elementare Gefährdung	Eintritt	Schaden	Risiko	Bemerkung
G 0.14 Ausspähen von Informationen / Spionage	mittel	hoch	mittel	
G 0.16 Diebstahl von Geräten, Datenträgern oder Dokumenten	mittel	hoch	mittel	
G 0.18 Fehlplanung oder fehlende Anpassung		gering	tragbar	indirekt
G 0.19 Offenlegung schützenswerter Informationen	mittel	hoch	mittel	
G 0.20 Informationen oder Produkte aus unzuverlässiger Quelle	gering	gering	tragbar	indirekt
G 0.21 Manipulation von Hard- oder Software	gering	gering	tragbar	indirekt
G 0.22 Manipulation von Informationen	gering	gering	tragbar	betrifft nur Integrität
G 0.23 Unbefugtes Eindringen in IT-Systeme	mittel	hoch	mittel	Zugang impliziert nicht automatisch Zugriff, dennoch grundlegend
G 0.25 Ausfall von Geräten oder Systemen	-	-	-	-
G 0.26 Fehlfunktion von Geräten oder Systemen	mittel	gering	tragbar	indirekt
G 0.27 Ressourcenmangel		gering	tragbar	indirekt
G 0.28 Software-Schwachstellen oder –Fehler	mittel	gering	tragbar	indirekt
G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen	gering	hoch	tragbar	indirekt
G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen	gering	gering	tragbar	indirekt
G 0.32 Missbrauch von Berechtigungen	mitel	hoch	mittel	Indirekt aber grundlegend

Tabelle 10: Bewertung der elementaren Gefährdung zu SYS.1.1 Allgemeiner Server für den 1. Risikobereich VPP

Den Anforderungen im Baustein **SYS.2.1 Allgemeiner Client** (modelliert für SYS-CC-4 EMS User Interface) sind elementare Gefährdungen zugeordnet, die wie folgt hinsichtlich des Risikobereichs „Verlust von Vertraulichkeit (Schwerpunkt), Integrität und Authentizität (besonderer) personenbezogener Daten“ bewertet werden:

Elementare Gefährdung	Eintritt	Schaden	Risiko	Bemerkung
G 0.14 Ausspähen von Informationen / Spionage	mittel	hoch	mittel	
G 0.15 Abhören	mittel	hoch	mittel	Indirekt (bezieht sich auf das LAN)
G 0.16 Diebstahl von Geräten, Datenträgern oder Dokumenten	mittel	hoch	mittel	
G 0.19 Offenlegung schützenswerter Informationen	mittel	hoch	mittel	
G 0.20 Informationen oder Produkte aus unzuverlässiger Quelle	gering	gering	tragbar	indirekt
G 0.21 Manipulation von Hard- oder Software	mittel	gering	tragbar	indirekt
G 0.22 Manipulation von Informationen	gering	gering	tragbar	betrifft nur Integrität
G 0.23 Unbefugtes Eindringen in IT-Systeme	mittel	hoch	mittel	Zugang impliziert nicht automatisch Zugriff, dennoch grundlegend
G 0.25 Ausfall von Geräten oder Systemen	-	-	-	-
G 0.26 Fehlfunktion von Geräten oder Systemen	mittel	gering	tragbar	indirekt
G 0.28 Software-Schwachstellen oder -Fehler	mittel	gering	tragbar	indirekt
G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen	mittel	gering	tragbar	indirekt
G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen	mittel	gering	tragbar	indirekt
G 0.36 Identitätsdiebstahl	mittel	hoch	mittel	Indirekt aber grundlegend
G 0.39 Schadprogramme	mittel	gering	tragbar	Indirekt

Elementare Gefährdung	Eintritt	Schaden	Risiko	Bemerkung
G 0.40 Verhinderung von Diensten (Denial of Service)	-	-	-	-
G 0.43 Einspielen von Nachrichten	gering	gering	tragbar	betrifft nur Integrität
G 0.45 Datenverlust	-	-	-	-
G 0.46 Integritätsverlust schützenswerter Informationen	gering	gering	tragbar	betrifft nur Integrität

Tabelle 11: Bewertung der elementaren Gefährdung zu SYS.2.1 Allgemeiner Client für den 1. Risikobereich VPP

Den Anforderungen im Baustein **NET.1.1 Netzarchitektur und -design** (modelliert für NET-CC-4 Intracenter Integration Bus) sind elementare Gefährdungen zugeordnet, die wie folgt hinsichtlich des Risikobereichs „Verlust von Vertraulichkeit (Schwerpunkt), Integrität und Authentizität (besonderer) personenbezogener Daten“ bewertet werden:

Elementare Gefährdung	Eintritt	Schaden	Risiko	Bemerkung
G 0.9 Ausfall oder Störung von Kommunikationsnetzen	gering	gering	tragbar	indirekt
G 0.11 Ausfall oder Störung von Dienstleistern	-	-	-	-
G 0.18 Fehlplanung oder fehlende Anpassung	gering	gering	tragbar	indirekt
G 0.19 Offenlegung schützenswerter Informationen	mittel	hoch	mittel	
G 0.22 Manipulation von Informationen		gering	tragbar	betrifft nur Integrität
G 0.23 Unbefugtes Eindringen in IT-Systeme	mittel	hoch	mittel	Zugang impliziert nicht automatisch Zugriff, dennoch grundlegend
G 0.27 Ressourcenmangel		gering	tragbar	indirekt
G 0.29 Verstoß gegen Gesetze oder Regelungen	mittel	hoch	mittel	Umgang mit personenbezogenen Daten ist in Deutschland über eine Vielzahl von Vorschriften geregelt.
G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen	gering	hoch	tragbar	indirekt
G 0.39 Schadprogramme	gering	hoch	tragbar	indirekt
G 0.40 Verhinderung von Diensten (Denial of Service)	-	-	-	-
G 0.43 Einspielen von Nachrichten	gering	gering	tragbar	betrifft nur Integrität

Tabelle 12: Bewertung der elementaren Gefährdung zu NET.1.1 Netzarchitektur und -design für den 1. Risikobereich VPP

Den Anforderungen im Baustein **INF.2 Rechenzentrum sowie Serverraum** (modelliert für INF-CC-2 Serverraum im Unternehmensgebäude) sind elementare Gefährdungen zugeordnet, die wie folgt hinsichtlich des Risikobereichs „Verlust von Vertraulichkeit (Schwerpunkt), Integrität und Authentizität (besonderer) personenbezogener Daten“ bewertet werden:

Elementare Gefährdung	Eintritt	Schaden	Risiko	Bemerkung
G 0.1 Feuer	-	-	-	-
G 0.2 Ungünstige klimatische Bedingungen	-	-	-	-
G 0.3 Wasser	-	-	-	-
G 0.4 Verschmutzung, Staub, Korrosion	-	-	-	-
G 0.5 Naturkatastrophen	-	-	-	-
G 0.6 Katastrophen im Umfeld	-	-	-	-
G 0.7 Großereignisse im Umfeld	-	-	-	-

Elementare Gefährdung	Eintritt	Schaden	Risiko	Bemerkung
G 0.8 Ausfall oder Störung der Stromversorgung	-	-	-	-
G 0.10 Ausfall oder Störung von Versorgungsnetzen	-	-	-	-
G 0.11 Ausfall oder Störung von Dienstleistern	-	-	-	-
G 0.14 Ausspähen von Informationen / Spionage	mittel	hoch	mittel	Betroffen wären z. B. PIN zum Betreten des Raumes, potenziell hoher Schaden, wenn der Angriff fortgeführt werden kann.
G 0.15 Abhören	gering	hoch	tragbar	Indirekt (abgehört werden würde ein Netz, kein Raum)
G 0.24 Zerstörung von Geräten oder Datenträgern	-	-	-	-
G 0.25 Ausfall von Geräten oder Systemen	-	-	-	-
G 0.26 Fehlfunktion von Geräten oder Systemen	mittel	gering	tragbar	indirekt
G 0.29 Verstoß gegen Gesetze oder Regelungen	mittel	hoch	mittel	Potenziell hoher Schaden, wenn der Angriff fortgeführt werden kann, so dass schließlich personenbezogene Daten betroffen wären.
G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen	gering	gering	tragbar	indirekt
G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen	gering	gering	tragbar	indirekt
G 0.32 Missbrauch von Berechtigungen	mittel	hoch	mittel	Betroffen wären z. B. PIN zum Betreten des Raumes, potenziell hoher Schaden, wenn der Angriff fortgeführt werden kann.
G 0.33 Personalausfall	-	-	-	-
G 0.34 Anschlag	-	-	-	-
G 0.41 Sabotage	-	-	-	-
G 0.44 Unbefugtes Eindringen in Räumlichkeiten	mittel	hoch	mittel	Potenziell hoher Schaden, wenn der Angriff fortgeführt werden kann.

Tabelle 13: Bewertung der elementaren Gefährdung zu INF.2 Rechenzentrum sowie Serverraum für den 1. Risikobereich VPP

Den Anforderungen im Baustein **INF.7 Büroarbeitsplatz** (modelliert für INF-CC-3 Warteraum im Unternehmensgebäude) sind elementare Gefährdungen zugeordnet, die wie folgt hinsichtlich des Risikobereichs „Verlust von Vertraulichkeit (Schwerpunkt), Integrität und Authentizität (besonderer) personenbezogener Daten“ bewertet werden:

Elementare Gefährdung	Eintritt	Schaden	Risiko	Bemerkung
G 0.2 Ungünstige klimatische Bedingungen	-	-	-	-
G 0.13 Abfangen kompromittierender Strahlung	gering	hoch	tragbar	Es erscheint unwahrscheinlich, dass ein derartig hoher Aufwand vom Angreifer betrieben wird.
G 0.14 Ausspähen von Informationen / Spionage	mittel	hoch	mittel	Betroffen wären z. B. PIN zum Betreten des Raume, potenziell hoher Schaden,

Elementare Gefährdung	Eintritt	Schaden	Risiko	Bemerkung
				wenn der Angriff fortgeführt werden kann.
G 0.15 Abhören	gering	hoch	tragbar	Indirekt (abgehört werden würde ein Netz, keine Raum)
G 0.16 Diebstahl von Geräten, Datenträgern oder Dokumenten	mittel	hoch	mittel	
G 0.18 Fehlplanung oder fehlende Anpassung	gering	gering	tragbar	indirekt
G 0.21 Manipulation von Hard- oder Software	gering	gering	tragbar	betrifft nur Integrität
G 0.22 Manipulation von Informationen	gering	gering	tragbar	betrifft nur Integrität
G 0.23 Unbefugtes Eindringen in IT-Systeme	gering	gering	tragbar	indirekt
G 0.24 Zerstörung von Geräten oder Datenträgern	-	-	-	-
G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen	gering	gering	tragbar	indirekt
G 0.44 Unbefugtes Eindringen in Räumlichkeiten	mittel	hoch	mittel	Potenziell hoher Schaden, wenn der Angriff fortgeführt werden kann.
G 0.46 Integritätsverlust schützenswerter Informationen	gering	gering	tragbar	betrifft nur Integrität

Tabelle 14: Bewertung der elementaren Gefährdung zu INF.7 Büroarbeitsplatz für den 1. Risikobereich VPP

Den Anforderungen im Baustein **INF.1 Allgemeines Gebäude** (modelliert für INF-CC-1 Unternehmensgebäude) sind elementare Gefährdungen zugeordnet, die wie folgt hinsichtlich des Risikobereichs „Verlust von Vertraulichkeit (Schwerpunkt), Integrität und Authentizität (besonderer) personenbezogener Daten“ bewertet werden:

Elementare Gefährdung	Eintritt	Schaden	Risiko	Bemerkung
G 0.1 Feuer	-	-	-	-
G 0.2 Ungünstige klimatische Bedingungen	-	-	-	-
G 0.3 Wasser	-	-	-	-
G 0.4 Verschmutzung, Staub, Korrosion	-	-	-	-
G 0.5 Naturkatastrophen	-	-	-	-
G 0.6 Katastrophen im Umfeld	-	-	-	-
G 0.7 Großereignisse im Umfeld	-	-	-	-
G 0.8 Ausfall oder Störung der Stromversorgung	-	-	-	-
G 0.10 Ausfall oder Störung von Versorgungsnetzen	-	-	-	-
G 0.16 Diebstahl von Geräten, Datenträgern oder Dokumenten	mittel	hoch	mittel	Potenziell hoher Schaden, wenn der Angriff fortgeführt werden kann, so dass schließlich personenbezogene Daten betroffen wären.
G 0.18 Fehlplanung oder fehlende Anpassung	mittel	gering	tragbar	indirekt
G 0.29 Verstoß gegen Gesetze oder Regelungen	mittel	hoch	mittel	Potenziell hoher Schaden, wenn der Angriff fortgeführt werden kann, so dass schließlich personenbezogene Daten betroffen wären.
G 0.34 Anschlag	-	-	-	-

Elementare Gefährdung	Eintritt	Schaden	Risiko	Bemerkung
G 0.44 Unbefugtes Eindringen in Räumlichkeiten	mittel	hoch	mittel	Potenziell hoher Schaden, wenn der Angriff fortgeführt werden kann.

Tabelle 15: Bewertung der elementaren Gefährdung zu INF.1 Allgemeines Gebäude für den 1. Risikobereich VPP

Betrachtung im Zusammenhang

		Wirkung auf					
Elementare Gefährdung	EMS ANW-1	EMS SYS-CC-2	EMS UI SYS-CC-2	ICI Bus NET-CC-4	Raum Srv INF-CC-2	Warte INF-CC-3	Geb. INF-CC-1
G 0.14 Ausspähen von Informationen / Spionage		x	x		x	x	
G 0.15 Abhören	x						x
G 0.16 Diebstahl von Geräten, Datenträgern oder Dokumenten		x	x			x	x
G 0.19 Offenlegung schützenswerter Informationen		x	x	x			
G 0.21 Manipulation von Hard- oder Software	x						
G 0.23 Unbefugtes Eindringen in IT-Systeme		x	x	x			
G 0.28 Software-Schwachstellen oder –Fehler	x						
G 0.29 Verstoß gegen Gesetze oder Regelungen				x	x		x
G 0.32 Missbrauch von Berechtigungen		x			x		
G 0.36 Identitätsdiebstahl			x				
G 0.44 Unbefugtes Eindringen in Räumlichkeiten					x	x	x

Tabelle 16: Alle als relevant bewerteten elementaren Gefährdungen für den 1. Risikobereich VPP

Risiken:

Angriff	Bewertung vorausges. ITGS-Anf. sind umgesetzt	Zusätzliche Maßnahme(n)
Nach unbefugtem **Eindringen** (zunächst in das Gebäude, dann in einen Raum) werden Systeme, Datenträger oder Dokumente **gestohlen**, auf denen sich für den Angreifer lesbare personenbezogene Daten in relevantem Umfang befinden.	Tragbar (zweifache Zutrittskontrolle)	-
Durch **Innentäter** werden Systeme, Datenträger oder Dokumente **gestohlen**, auf denen sich für	Mittel	Verschlüsselung von Datenträgern und Notebooks

Angriff	Bewertung vorausges. ITGS-Anf. sind umgesetzt	Zusätzliche Maßnahme(n)
den Angreifer lesbare personenbezogene Daten in relevantem Umfang befinden.		
Nach unbefugtem **Eindringen** (zunächst in das Gebäude, dann in einen Raum) kann sich ein Angreifer Zugriff auf das Netz verschaffen und den **Datenverkehr mitlesen** mit für ihn lesbaren personenbezogenen Daten in relevantem Umfang.	Tragbar Für einen erfolgreichen Angriff müssten mehrere Sicherheitsmaßnahmen überwunden werden: Zutrittskontrollen Gebäude / Raum und Netzwerkkontrollen.	-
Nach unbefugtem **Eindringen** (zunächst in das Gebäude, dann in einen Raum) kann ein Angreifer **Zugang zu einem System** mit für ihn lesbaren personenbezogenen Daten in relevantem Umfang erlangen. Dabei nutzt er Schwachstellen der Software aus und / oder führt Manipulationen an der Software durch.	Tragbar (zweifache Zutrittskontrolle, wirksame Zugangskontrolle)	-
Ein Angreifer kann über das **Internet** in das Netz und weiter in die Systeme **eindringen** und für ihn lesbare personenbezogene Daten in relevantem Umfang abgreifen.	Tragbar, falls alle Netzschnittstellen durch wirksame Sicherheitsgateways geschützt sind.	
Ein **Innentäter** kann seine **Rechte missbrauchen** und außerhalb des bestimmungsmäßigen Gebrauchs für ihn lesbare personenbezogene Daten in relevantem Umfang abgreifen. Dabei nutzt er Schwachstellen der Software aus und / oder führt Manipulationen an der Software durch.	Wenn ein Rollenmodell und least privilege konsequent umgesetzt sind, dann liegt maximal ein mittleres Risiko vor.	Sicherheitsüberprüfung des Personals, evaluierte Software

Tabelle 17: Risiken für den 1. Risikobereich VPP

8.2.1.2 „Smart Metering“ (2. Risikobereich VPP)

Die an diesem Prozess beteiligten Assets sind in Tabelle 18 aufgelistet.
Im Zusammenhang mit Smart Metering werden personenbezogene Verbrauchsdaten verarbeitet und übertragen. Diese haben einen hohen Schutzbedarf der Vertraulichkeit, der sich auf die beteiligten Assets überträgt.
SMGW sind durch IT-Grundschutzbausteine nur unzureichend modellierbar.

Assets in Scope 06 - Virtuelles Kraftwerk Geschäftsprozess „Smart Metering“			
Typ	**Bezeichnung**	**ID**	**Baustein(e)**
System / Gerät	Internal Smart Meter Gateway	IND-Pros-1	NET.3.1
System / Gerät	External Smart Meter Gateway	SYS-Pros-1	NET.3.1 *Abdeckung nicht ausreichend*
Infrastruktur	Zählerkasten zur Prosumer-DER-Anlage (z. B. im Wohnhaus; enthält External Smart Meter Gateway, Internal Smart Meter Gateway, Customer Energy Management)	INF-Pros-1	*keine Abdeckung durch Baustein*

Assets in Scope 06 - Virtuelles Kraftwerk Geschäftsprozess „Smart Metering“			
Typ	**Bezeichnung**	**ID**	**Baustein(e)**
Netz / Kommunikati-onsverbindung	Verbindung External SMGW zum Smart Metering (via AMI Backhaul Network)	NET-1-AV1	NET.1.1 NET.3.3
Netz / Kommunikati-onsverbindung	Verbindung External SMGW zur Leitwarte (via AMI Backhaul Network und Backbone Network (realisie-rungsabhängig, z. B. Internet mit Umsetzer dazwischen)	NET-1/6-AV2	NET.1.1 NET.3.3
Netz / Kommunikati-onsverbindung	Verbindung Leitwarte zum Smart Metering (via Backbone Network (z. B. Internet))	NET-6-AV3	NET.1.1 NET.3.3
Netz / Kommunikati-onsverbindung	Verbindung zwischen Home & Building Integration Bus und CEM User Interface (letzteres ist nicht im IV)	NET-2-AV1	NET.1.1
Netz / Kommunikati-onsverbindung	Verbindung zwischen External SMGW und MID Meter 2 (letzteres ist nicht im IV)	NET-7-AV1	NET.1.1

Tabelle 18: Assets zum Smart Metering

Den Anforderungen in den IT-Grundschutz-Bausteinen sind jeweils elementare Gefährdungen zugeordnet. Diese werden in den folgenden Tabellen aufgelistet, ggf. ergänzt, und es werden jeweils Eintrittswahrscheinlichkeit und Schadenshöhe bewertet (die dabei verwendeten Skalen sind von den Verantwortlichen zuvor zu definieren) unter der Voraussetzung, dass die Grundschutzanforderungen erfüllt sind aber keine zusätzlichen Maßnahmen festgelegt wurden. Daraus wird das jeweilige Risiko abgeleitet. Bei der Bewertung wird berücksichtigt, dass der Schwerpunkt des Risikobereichs beim Verlust der Vertraulichkeit (besonderer) personenbezogener Daten liegt. Elementare Gefährdungen, die in Bezug auf den Risikobereich nicht relevant sind, erhalten keine Bewertung („ - “).

Den Anforderungen im Baustein **NET.3.1 Router und Switches** (modelliert für IND-Pros-1 Internal Smart Meter Gateway und External Smart Meter Gateway SYS-Pros-1) sind elementare Gefährdungen zugeordnet, die wie folgt hinsichtlich des Risikobereichs „Verlust von Vertraulichkeit (Schwerpunkt), Integrität und Authentizität (besonderer) personenbezogener Daten“ bewertet werden:

Elementare Gefährdung	Eintritt	Schaden	Risiko	Bemerkung
G 0.09 Ausfall oder Störung von Kommunikati-onsnetzen	-	-	-	-
G 0.11 Ausfall oder Störung von Dienstleistern	-	-	-	-
G 0.14 Ausspähen von Informationen (Spio-nage)	gering	hoch	mittel	
G 0.15 Abhören	mittel	hoch	mittel	
G 0.16 Diebstahl von Geräten, Datenträgern oder Dokumenten	gering	gering	tragbar	Indirekt (der Gefährdung wird durch Zutrittskon-trolle begegnet)
G 0.17 Verlust von Geräten, Datenträgern oder Dokumenten	-	-	-	-
G 0.18 Fehlplanung oder fehlende Anpassung	-	-	-	-
G 0.19 Offenlegung schützenswerter Informati-onen	mittel	hoch	mittel	
G 0.20 Informationen oder Produkte aus unzu-verlässiger Quelle	gering	gering	tragbar	Indirekt
G 0.21 Manipulation von Hard- oder Software	gering	gering	tragbar	Indirekt
G 0.22 Manipulation von Informationen	gering	gering	mittel	Betrifft die Integrität

Elementare Gefährdung	Eintritt	Schaden	Risiko	Bemerkung
G 0.23 Unbefugtes Eindringen in IT-Systeme	gering	hoch	mittel	Indirekt aber grundlegend
G 0.25 Ausfall von Geräten oder Systemen	-	-	-	-
G 0.26 Fehlfunktion von Geräten oder Systemen	mittel	gering	tragbar	Indirekt
G 0.27 Ressourcenmangel	-	-	-	-
G 0.28 Software-Schwachstellen oder -Fehler	mittel	gering	tragbar	Indirekt
G 0.29 Verstoß gegen Gesetze oder Regelungen		hoch	mittel	
G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen	gering	gering	tragbar	Indirekt
G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen	mittel	gering	tragbar	Indirekt
G 0.32 Missbrauch von Berechtigungen	mittel	hoch	mittel	
G 0.36 Identitätsdiebstahl	gering	gering	tragbar	Indirekt
G 0.37 Abstreiten von Handlungen	gering	gering	tragbar	Indirekt
G 0.38 Missbrauch personenbezogener Daten	mittel	hoch	mittel	
G 0.40 Verhinderung von Diensten (Denial of Service)	-	-	-	-
G 0.42 Social Engineering	mittel	gering	mittel	Indirekt
G 0.43 Einspielen von Nachrichten	gering	gering	tragbar	Betrifft die Integrität
G 0.45 Datenverlust	-	-	-	-
G 0.46 Integritätsverlust schützenswerter Informationen	gering	hoch	mittel	Betrifft die Integrität

Tabelle 19: Bewertung der elementaren Gefährdung zu NET.3.1 Router und Switches für den 2. Risikobereich VPP

Der Baustein **NET.1.1 Netzarchitektur und -design** wurde modelliert für:

- NET-1-AV1 Verbindung External SMGW zum Smart Metering
- NET-1/6-AV2 Verbindung External SMGW zur Leitwarte
- NET-6-AV3 Verbindung Leitwarte zum Smart Metering
- NET-2-AV1 Verbindung zwischen Home & Building Integration Bus und CEM User Interface
- NET-7-AV1 Verbindung zwischen External SMGW und MID Meter 2

Den Anforderungen sind elementare Gefährdungen zugeordnet, die wie folgt hinsichtlich des Risikobereichs „Verlust von Vertraulichkeit (Schwerpunkt), Integrität und Authentizität (besonderer) personenbezogener Daten“ bewertet werden:

Elementare Gefährdung	Eintritt	Schaden	Risiko	Bemerkung
G 0.9 Ausfall oder Störung von Kommunikationsnetzen	mittel	gering	tragbar	Indirekt
G 0.11 Ausfall oder Störung von Dienstleistern	-	-	-	-
G 0.18 Fehlplanung oder fehlende Anpassung	mittel	gering	tragbar	Indirekt
G 0.19 Offenlegung schützenswerter Informationen	gering	hoch	mittel	
G 0.22 Manipulation von Informationen	k.A.	gering	tragbar	Betrifft nur Integrität
G 0.23 Unbefugtes Eindringen in IT-Systeme	gering	hoch	mittel	Zugang impliziert nicht automatisch Zugriff, dennoch grundlegend.
G 0.27 Ressourcenmangel	gering	gering	tragbar	Indirekt
G 0.29 Verstoß gegen Gesetze oder Regelungen	k.A.	hoch	mittel	Umgang mit personenbezogenen Daten ist in Deutschland über eine Vielzahl von Vorschriften geregelt.

Elementare Gefährdung	Eintritt	Schaden	Risiko	Bemerkung
G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen	gering	hoch	tragbar	Indirekt
G 0.39 Schadprogramme	gering	hoch	tragbar	Indirekt
G 0.40 Verhinderung von Diensten (Denial of Service)	-	-	-	-
G 0.43 Einspielen von Nachrichten	gering	gering	tragbar	Betrifft nur Integrität
Ggf. zusätzliche relevante Gefährdungen				

Tabelle 20: Bewertung der elementaren Gefährdung zu NET.1.1 Netzarchitektur und -design für den 2. Risikobereich VPP

Der zwischenzeitlich als sog. Community Draft (CD) vorgelegte **Baustein INF.5 Raum oder Schrank für technische Infrastruktur (CD)**[1] wurde bisher noch nicht modelliert für INF-Pros-1 Zählerkasten zur Prosumer-DER-Anlage. Die elementaren Gefährdungen, die den darin enthaltenen Anforderungen zugeordnet sind bzw. waren, können jedoch als Ausgangspunkt für eine Risikoanalyse hinsichtlich der noch nicht ausreichenden Abdeckung des Assets INF-Pros-1 dienen. Sie werden hinsichtlich des Risikobereichs „Verlust von Vertraulichkeit (Schwerpunkt), Integrität und Authentizität (besonderer) personenbezogener Daten“ wie folgt bewertet:

Elementare Gefährdung	Eintritt	Schaden	Risiko	Bemerkung
G 0.01 Feuer	-	-	-	-
G 0.02 Ungünstige klimatische Bedingungen	-	-	-	-
G 0.03 Wasser	-	-	-	
G 0.04 Verschmutzung, Staub, Korrosion	-	-	-	-
G 0.05 Naturkatastrophen	-	-	-	-
G 0.08 Ausfall oder Störung der Stromversorgung	-	-	-	-
G 0.10 Ausfall oder Störung von Versorgungsnetzen	-	-	-	-
G 0.11 Ausfall oder Störung von Dienstleistern	-	-	-	-
G 0.13 Abfangen kompromittierender Strahlung	gering	gering	tragbar	Der erforderliche Aufwand scheint in einem schlechten Verhältnis zum böswilligen Effekt zu stehen.
G 0.18 Fehlplanung oder fehlende Anpassung	-	-	-	-
G 0.24 Zerstörung von Geräten oder Datenträgern	-	-	-	-
G 0.25 Ausfall von Geräten oder Systemen	-	-	-	-
G 0.26 Fehlfunktion von Geräten oder Systemen	-	-	-	-
G 0.29 Verstoß gegen Gesetze oder Regelungen	gering	hoch	tragbar	Indirekt
G 0.33 Personalausfall	-	-	-	-
G 0.41 Sabotage	-	-	-	-
G 0.44 Unbefugtes Eindringen in Räumlichkeiten	mittel	hoch	mittel	Unbefugtes Eindringen bzw. öffnen könnte erster Schritt in einem Spionage/Sabotage Angriff sein.

Tabelle 21: Bewertung der elementaren Gefährdung zu INF.5 Raum oder Schrank für technische Infrastruktur (CD) für den 2. Risikobereich VPP

[1] Seitens BSI gibt es hierzu aktuell die Aussage, dass dieser Baustein demnächst als überarbeiteter CD erneut veröffentlicht und in die Edition 2020 des ITGS-Kompendiums aufgenommen werden soll.

Den Anforderungen im Baustein **NET.3.3 VPN** wurde modelliert für

- NET-1-AV1 Verbindung External SMGW zum Smart Metering
- NET-1 / 6-AV2 Verbindung External SMGW zur Leitwarte
- NET-6-AV3 Verbindung Leitwarte zum Smart Metering)

sind elementare Gefährdungen zugeordnet, die wie folgt hinsichtlich des Risikobereichs „Verlust von Vertraulichkeit (Schwerpunkt), Integrität und Authentizität (besonderer) personenbezogener Daten“ bewertet werden:

Elementare Gefährdung	Eintritt	Schaden	Risiko	Bemerkung
G 0.09 Ausfall oder Störung von Kommunikationsnetzen	-	-	-	-
G 0.11 Ausfall oder Störung von Dienstleistern	-	-	-	-
G 0.14 Ausspähen von Informationen (Spionage)	gering	hoch	mittel	
G 0.18 Fehlplanung oder fehlende Anpassung	-	-	-	-
G 0.19 Offenlegung schützenswerter Informationen	gering	hoch	mittel	
G 0.22 Manipulation von Informationen	gering	hoch	tragbar	Betrifft die Integrität
G 0.23 Unbefugtes Eindringen in IT-Systeme	gering	hoch	mittel	Indirekt, Zugang impliziert nicht automatisch Zugriff
G 0.28 Software-Schwachstellen oder -Fehler	mittel	gering	mittel	Indirekt
G 0.32 Missbrauch von Berechtigungen	gering	hoch	mittel	
G 0.40 Verhinderung von Diensten (Denial of Service)	-	-	-	-
G 0.43 Einspielen von Nachrichten	gering	hoch	tragbar	Betrifft die Integrität
G 0.46 Integritätsverlust schützenswerter Informationen	gering	hoch	tragbar	Betrifft die Integrität

Tabelle 22: Bewertung der elementaren Gefährdung zu NET.3.3 VPN für den 2. Risikobereich VPP

Betrachtung im Zusammenhang

	Wirkung auf					
Elementare Gefährdung	Int SMGW IND-Pros-1	Ext. SMGW SYS-Pros-1	Zählerk. INF-Pros-1	Verb. SMGW NET-1-AV1 NET-1 / 6-AV2 NET-6-AV3	weitere-Verb. NET-2-AV1 NET-7-AV1	
G 0.14 Ausspähen von Informationen (Spionage)	x	x		x		
G 0.15 Abhören	x	x				
G 0.19 Offenlegung schützenswerter Informationen	x	x		x	x	
G 0.23 Unbefugtes Eindringen in IT-Systeme	x	x		x	x	
G 0.29 Verstoß gegen Gesetze oder Regelungen	x	x		x	x	
G 0.32 Missbrauch von Berechtigungen	x	x		x		
G 0.38 Missbrauch personenbezogener Daten	x	x				
G 0.44 Unbefugtes Eindringen in Räumlichkeiten			x			

Tabelle 23: Alle als relevant bewerteten elementaren Gefährdungen für den 2. Risikobereich VPP

Risiken:

Angriff	**Bewertung vorausges. ITGS-Anf. sind umgesetzt**	**Zusätzliche Maßnahme(n)**
Abhören und auswerten der Kommunikation zwischen • NET-1-AV1 Verbindung External SMGW zum Smart Metering • NET-1 / 6-AV2 Verbindung External SMGW zur Leitwarte • NET-6-AV3 Verbindung Leitwarte zum Smart Metering zur Sammlung personenbezogener Daten	Das Risiko ist tragbar, da die Verbindungen als VPN realisiert sind. Außerdem wären nur Daten in bestimmten Zeiträumen betroffen.	keine
Abhören und auswerten der Kommunikation zwischen • NET-2-AV1 Verbindung zwischen Home & Building Integration Bus und CEM User Interface • NET-7-AV1 Verbindung zwischen External SMGW und MID Meter 2 zur Sammlung personenbezogener Daten	Falls die Kommunikation nicht kryptografisch geschützt verläuft und die Schnittstellen physisch zugreifbar sind, könnten lokal personenbezogene Daten abgefangen werden.	Die Kommunikationsverbindungen und Schnittstellen sind logisch (Verschlüsselung) oder durch physische Absicherung zu schützen.
Zugang eines Unberechtigten zum „Internal Smart Meter Gateway IND-Pros-1“ und Zugriff auf personenbezogene Daten	Im Falle von zu schwacher physischer Zugriffskontrolle und mangelndem Einbruchschutz kann ein nicht tragbares Risiko vorliegen.	Die im vorübergehend vorliegenden CD INF.5 formulierten Anforderungen „INF.5.A3 Zutrittsregelung und -kontrolle“ und „INF.5.A20 Schutz vor Einbruch und Sabotage“ sind wirksam umzusetzen.
Zugang eines Unberechtigten zum „External Smart Meter Gateway SYS-Pros-1“ und Zugriff auf personenbezogene Daten	Im Falle von zu schwacher physischer Zugriffskontrolle und mangelndem Einbruchschutz kann ein nicht tragbares Risiko vorliegen.	Die im vorübergehend vorliegenden CD INF.5 formulierten Anforderungen „INF.5.A3 Zutrittsregelung und -kontrolle“ und „INF.5.A20 Schutz vor Einbruch und Sabotage“ sind wirksam umzusetzen.

Tabelle 24: Risiken für den 2. Risikobereich VPP

8.2.2 Risikobereich „Verlust der Integrität (Schwerpunkt), Authentizität und Verfügbarkeit von Kontroll- und Steuerungsdaten und -funktionen“

Die korrekte Übermittlung von Steuerbefehlen und Daten zwischen der Leitwarte und den dezentralen Einrichtungen ist eine Grundvoraussetzung für den Betrieb eines virtuellen Kraftwerks.
Die verteilten Energieerzeugungsanlagen müssen mit der Leitwarte des virtuellen Kraftwerks vernetzt werden. Die dafür notwendigen Kommunikations-Gateways müssen mit der SPS der Anlage vor Ort sowie mit der Leitwarte kommunizieren.
Im Falle des hier modellierten virtuellen Kraftwerks wird zwischen der netzgebundenen DER-Anlage (Grid connected DER plant) und der Prosumer-DER-Anlage (Prosumer DER plant) unterschieden. Bei ersterem ist „SYS-DER-1 DER Gateway“ die zentrale Kommunikationskomponente, bei letzterem „SYS-Pros-1 External Smart Meter Gateway“.
Die korrekte Übermittlung und Verarbeitung der Steuerbefehle ist in beiden Ausprägungen eine kritische Funktionalität.

8.2.2.1 Risiken im Zusammenhang mit SYS-DER-1 DER Gateway

In diesem Risikobereich werden die Integrität des DER Gateway SYS-DER-1 und der Kommunikation zwischen Leitwarte (Endpunkt Firewall) und DER Gateway sowie innerhalb des DER Integration Bus NET-DER-3 betrachtet.

Den Anforderungen im Baustein **NET.3.1 Router und Switches** (modelliert für DER Gateway SYS-DER-1) sind elementare Gefährdungen zugeordnet, die wie folgt hinsichtlich des Risikobereichs „Verlust der Integrität (Schwerpunkt), Authentizität und Verfügbarkeit von Kontroll- und Steuerungsdaten und -funktionen“ bewertet werden:

Elementare Gefährdung	Eintritt	Schaden	Risiko	Bemerkung
G 0.09 Ausfall oder Störung von Kommunikationsnetzen	-	-	-	-
G 0.11 Ausfall oder Störung von Dienstleistern	-	-	-	-
G 0.14 Ausspähen von Informationen (Spionage)	-	-	-	-
G 0.15 Abhören	-	-	-	-
G 0.16 Diebstahl von Geräten, Datenträgern oder Dokumenten	gering	gering	tragbar	Indirekt (der Gefährdung wird durch Zutrittskontrolle begegnet)
G 0.17 Verlust von Geräten, Datenträgern oder Dokumenten	gering	gering	tragbar	Indirekt
G 0.18 Fehlplanung oder fehlende Anpassung	-	-	-	-
G 0.19 Offenlegung schützenswerter Informationen	-	-	-	-
G 0.20 Informationen oder Produkte aus unzuverlässiger Quelle	mittel	hoch	mittel	Indirekt aber grundlegend
G 0.21 Manipulation von Hard- oder Software	mittel	hoch	mittel	Indirekt aber grundlegend
G 0.22 Manipulation von Informationen	mittel	hoch	mittel	
G 0.23 Unbefugtes Eindringen in IT-Systeme	mittel	mittel	mittel	Indirekt aber grundlegend
G 0.25 Ausfall von Geräten oder Systemen	mittel	gering	tragbar	Verfügbarkeitsverlust wäre lokal begrenzt
G 0.26 Fehlfunktion von Geräten oder Systemen	mittel	gering	tragbar	
G 0.27 Ressourcenmangel	gering	gering	tragbar	Indirekt
G 0.28 Software-Schwachstellen oder -Fehler	mittel	hoch	mittel	Indirekt
G 0.29 Verstoß gegen Gesetze oder Regelungen	-	-	-	-

Elementare Gefährdung	Eintritt	Schaden	Risiko	Bemerkung
G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen	mittel	hoch	mittel	Indirekt
G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen	mittel	gering	tragbar	Indirekt
G 0.32 Missbrauch von Berechtigungen	mittel	hoch	mittel	Indirekt aber grundlegend
G 0.36 Identitätsdiebstahl	mittel	hoch	mittel	Indirekt
G 0.37 Abstreiten von Handlungen	mittel	gering	tragbar	Indirekt
G 0.38 Missbrauch personenbezogener Daten	-	-	-	
G 0.40 Verhinderung von Diensten (Denial of Service)	mittel	gering	tragbar	Verfügbarkeitsverlust wäre lokal begrenzt.
G 0.42 Social Engineering	mittel	gering	tragbar	Indirekt
G 0.43 Einspielen von Nachrichten	mittel	hoch	mittel	
mittel	mittel	mittel	tragbar	Verfügbarkeitsverlust wäre lokal begrenzt.
G 0.46 Integritätsverlust schützenswerter Informationen	mittel	sehr hoch	untragbar	

Tabelle 25: Bewertung der elementaren Gefährdung zu NET.3.1 Router und Switches für den 3. Risikobereich VPP

Den Anforderungen im Baustein **NET.1.1 Netzarchitektur und -design** (modelliert für DER Integration Bus NET-DER-3 und Operator Backhaul Network NET-5) sind elementare Gefährdungen zugeordnet, die wie folgt hinsichtlich des Risikobereichs „Verlust der Integrität (Schwerpunkt), Authentizität und Verfügbarkeit von Kontroll- und Steuerungsdaten und -funktionen“ bewertet werden:

Elementare Gefährdung	Eintritt	Schaden	Risiko	Bemerkung
G 0.9 Ausfall oder Störung von Kommunikationsnetzen	mittel	gering	tragbar	Betrifft nur die Verfügbarkeit
G 0.11 Ausfall oder Störung von Dienstleistern	mittel	gering	tragbar	Indirekt
G 0.18 Fehlplanung oder fehlende Anpassung	mittel	gering	tragbar	Indirekt
G 0.19 Offenlegung schützenswerter Informationen	-	-	-	-
G 0.22 Manipulation von Informationen	mittel	hoch	mittel	
G 0.23 Unbefugtes Eindringen in IT-Systeme	mittel	hoch	mittel	Zugang impliziert nicht automatisch Zugriff, dennoch grundlegend.
G 0.27 Ressourcenmangel	gering	gering	tragbar	Indirekt
G 0.29 Verstoß gegen Gesetze oder Regelungen	gering	gering	tragbar	Indirekt
G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen	mittel	hoch	mittel	Indirekt
G 0.39 Schadprogramme	mittel	hoch	mittel	Indirekt
G 0.40 Verhinderung von Diensten (Denial of Service)	mittel	gering	tragbar	Betrifft nur die Verfügbarkeit
G 0.43 Einspielen von Nachrichten	mittel	hoch	mittel	

Tabelle 26: Bewertung der elementaren Gefährdung zu NET.1.1 Netzarchitektur und –design für den 3. Risikobereich VPP

Den Anforderungen im Baustein **NET.3.3 VPN** (modelliert für Operator Backhaul Network NET-5) sind elementare Gefährdungen zugeordnet, die wie folgt hinsichtlich des Risikobereichs „Verlust der Integrität (Schwerpunkt), Authentizität und Verfügbarkeit von Kontroll- und Steuerungsdaten und -funktionen“ bewertet werden:

Elementare Gefährdung	Eintritt	Schaden	Risiko	Bemerkung
G 0.09 Ausfall oder Störung von Kommunikationsnetzen	gering	gering	tragbar	Betrifft nur die Verfügbarkeit.
G 0.11 Ausfall oder Störung von Dienstleistern	gering	gering	tragbar	Indirekt
G 0.14 Ausspähen von Informationen (Spionage)	-	-	-	-
G 0.18 Fehlplanung oder fehlende Anpassung	gering	gering	tragbar	Indirekt
G 0.19 Offenlegung schützenswerter Informationen	-	-	-	-
G 0.22 Manipulation von Informationen	mittel	hoch	mittel	
G 0.23 Unbefugtes Eindringen in IT-Systeme	mittel	hoch	mittel	Zugang impliziert nicht automatisch Zugriff, dennoch grundlegend.
G 0.28 Software-Schwachstellen oder -Fehler	mittel	gering	mittel	Indirekt
G 0.32 Missbrauch von Berechtigungen	gering	hoch	mittel	Indirekt
G 0.40 Verhinderung von Diensten (Denial of Service)	mittel	gering	tragbar	Betrifft nur die Verfügbarkeit
G 0.43 Einspielen von Nachrichten	mittel	hoch	mittel	
G 0.46 Integritätsverlust schützenswerter Informationen	mittel	sehr hoch	untragbar	

Tabelle 27: Bewertung der elementaren Gefährdung zu NET.3.3 VPN für den 3. Risikobereich VPP

Den Anforderungen im Baustein **NET.3.2 Firewall** (modelliert für Firewall Leitwarte SYS-CC-8) sind elementare Gefährdungen zugeordnet, die wie folgt hinsichtlich des Risikobereichs „Verlust der Integrität (Schwerpunkt), Authentizität und Verfügbarkeit von Kontroll- und Steuerungsdaten und -funktionen“ bewertet werden:

Elementare Gefährdung	Eintritt	Schaden	Risiko	Bemerkung
G 0.8 Ausfall oder Störung der Stromversorgung	gering	gering	tragbar	Indirekt
G 0.09 Ausfall oder Störung von Kommunikationsnetzen	gering	gering	tragbar	Indirekt
G 0.14 Ausspähen von Informationen (Spionage)	-	-	-	-
G 0.18 Fehlplanung oder fehlende Anpassung	gering	gering	tragbar	Indirekt
G 0.19 Offenlegung schützenswerter Informationen	-	-	-	-
G 0.20 Informationen oder Produkte aus unzuverlässiger Quelle	mittel	hoch	mittel	Indirekt aber grundlegend
G 0.21 Manipulation von Hard- oder Software	mittel	hoch	mittel	Indirekt aber grundlegend
G 0.22 Manipulation von Informationen	mittel	hoch	mittel	
G 0.23 Unbefugtes Eindringen in IT-Systeme	hoch	mittel	mittel	Indirekt aber grundlegend
G 0.24 Zerstörung von Geräten oder Datenträgern	gering	gering	tragbar	
G 0.25 Ausfall von Geräten oder Systemen	mittel	hoch	mittel	Verfügbarkeitsverlust einer zentralen Kommunikations-/ Sicherheitsinfrastruktur
G 0.26 Fehlfunktion von Geräten oder Systemen	mittel	hoch	mittel	Verfügbarkeitsverlust einer zentralen Kommunikations-/ Sicherheitsinfrastruktur
G 0.27 Ressourcenmangel	mittel	gering	tragbar	Indirekt

Elementare Gefährdung	Eintritt	Schaden	Risiko	Bemerkung
G 0.28 Software-Schwachstellen oder -Fehler	mittel	hoch	mittel	Indirekt
G 0.29 Verstoß gegen Gesetze oder Regelungen	-	-	-	-
G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen	mittel	hoch	mittel	Indirekt
G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen	mittel	gering	tragbar	Indirekt
G 0.32 Missbrauch von Berechtigungen	mittel	hoch	mittel	Indirekt aber grundlegend und es handelt sich um eine zentrale Sicherheitsinfrastruktur.
G 0.39 Schadprogramme	mittel	hoch	mittel	Indirekt
G 0.40 Verhinderung von Diensten (Denial of Service)	mittel	hoch	mittel	Verfügbarkeitsverlust einer zentralen Ko–Sicherheitsinfrastruktur
G 0.41 Sabotage	mittel	gering	tragbar	Indirekt
G 0.43 Einspielen von Nachrichten	mittel	hoch	mittel	
G 0.45 Datenverlust	gering	mittel	tragbar	
G 0.46 Integritätsverlust schützenswerter Informationen	mittel	sehr hoch	untragbar	

Tabelle 28: Bewertung der elementaren Gefährdung zu NET.3.2 Firewall für den 3. Risikobereich VPP

Betrachtung im Zusammenhang

	Wirkung auf			
Elementare Gefährdung	DER Gateway SYS-DER-1	DER Integration Bus NET-DER-3	Operator Backhaul Network NET-5	Firewall Leitwarte SYS-CC-8
G 0.20 Informationen oder Produkte aus unzuverlässiger Quelle	x			x
G 0.21 Manipulation von Hard- oder Software	x			x
G 0.22 Manipulation von Informationen	x	x	x	x
G 0.23 Unbefugtes Eindringen in IT-Systeme	x	x	x	x
G 0.25 Ausfall von Geräten oder Systemen				x
G 0.26 Fehlfunktion von Geräten oder Systemen				x
G 0.32 Missbrauch von Berechtigungen	x			x
G 0.40 Verhinderung von Diensten (Denial of Service)				x
G 0.43 Einspielen von Nachrichten	x	x	x	x
G 0.46 Integritätsverlust schützenswerter Informationen	x		x	x

Tabelle 29: Alle als relevant bewerteten elementaren Gefährdungen für den 3. Risikobereich VPP

Risiken:

Angriff	Bewertung voraus-ges. ITGS-Anf. sind umgesetzt	Zusätzliche Maßnahme(n)
Ausfall der oder DoS-Angriff auf die Firewall der Leitwarte	Das Risiko wird als mittel eingeschätzt, da keine Kommuni-kation zu allen de-zentralen Erzeugern und Verbrauchern möglich wäre.	Redundanzen
Penetration der Verbindung zwischen Leitwarte und dezentralen Einrichtungen und gezielte Verfäl-schung von Steuerbefehlen.	Die Verbindung ist als VPN realisiert. Das Ri-siko ist tragbar, wenn das VPN innerhalb ei-ner geschlossenen Benutzergruppe be-trieben wird und nicht per Internet er-reichbar ist.	
Penetration der Verbindungen innerhalb einer de-zentralen Einrichtung und gezielte Verfälschung von Steuerbefehlen.	Zum einen wird das Risiko dadurch be-grenzt, dass es sich um einen lokalen Vorfall handelt. Zum anderen wird durch die Basis-Anforde-rung NET.1.1.A7 be-reits Verschlüsselung und Authentisierung gefordert. Allerdings wird nicht explizit ein Integritätsschutz ge-fordert.	Starke Schutzmechanismen zur Sicherstellung der Integrität von Steuerbefehlen innerhalb der dezentralen Einrichtungen.
Zugang zum DER Gateway SYS-DER-1 und Zugriff auf Software, Konfiguration und Nutzdaten (Steu-erdaten und Statusdaten), Manipulation der Daten	Grundsätzlich wird dem Risiko durch Umsetzung der Grundschutzanfor-derungen begegnet. Ein Risiko besteht höchstens darin, das die Mechanismen zu schwach sind bzw. über die Zeit an Stärke verlieren.	Der Zugang zum Gateway darf nur nach Authentisierung mit starken Verfahren möglich sein. Es darf kein Zugang über Hintertüren möglich sein. Si-cherheitsrelevante Patches müssen zeitnah eingespielt werden. Ebenso muss es mög-lich sein, dass auf höherwertige Verfahren bzw. längerer Schlüssel migriert werden kann.

Tabelle 30: Risiken für den 3. Risikobereich VPP

8.2.2.2 Risiken im Zusammenhang mit SYS-Pros-1 External Smart Meter Gateway

Hinsichtlich der Kommunikation der Leitwarte mit dem SYS-Pros-1 External Smart Meter Gateway (4. Risikobereich VPP) und der Übertragung der Steuerdaten im lokalen Netzt beim Prosumer liegt grund-sätzlich die gleiche Gefährdungslage vor wie unter 8.2.2.1.

8.2.3 Risikobereich „Vorsätzliche Überwindung oder zufällige Schäden (einschließlich höherer Gewalt) bei Infrastruktureinrichtungen der dezentralen Erzeuger bzw. Verbraucher“

Zu diesem Risikobereich gehören die Zielobjekte

- INF-DER-1 Betriebsgelände DER-Anlage (enthält DER Equipment 1, z. B. Photovoltaik)
- INF-Pros-1 Zählerkasten zur Prosumer-DER-Anlage (z. B. im Wohnhaus; enthält External SMGW, Internal SMGW, Customer Energy Management)
- INF-Pros-2 Aufstellungsort Prosumer-DER-Anlage (z. B. Dach des Wohnhauses; Aufstellungsort für DER Equipment 2, z. B. Photovoltaik)

Bei der Risikoanalyse ist zwischen vorsätzlicher, fahrlässiger und zufälliger Zerstörung / Beeinträchtigung der Komponenten in der Infrastruktur und Überwindung von Zutritts- bzw. physischen Zugriffskontrollen als Vorbereitung für logische Angriffe zu unterscheiden.

Für „INF-DER-1 Betriebsgelände DER-Anlage“ und „INF-Pros-2 Aufstellungsort Prosumer-DER-Anlage“ existieren keine Bausteine. Die relevanten elementaren Gefährdungen werden daher unter der Annahme, dass noch keine Grundschutzanforderungen umgesetzt sind wie folgt bewertet:

Elementare Gefährdung	Eintritt	Schaden	Risiko	Bemerkung
G 0.1 Feuer	mittel	hoch	mittel	Die Auswirkungen des Vorfalls wären lokal begrenzt. Die sinngemäße Umsetzung von Basis- und Standardgrundschutzanforderungen zum Brandschutz reicht aus.
G 0.2 Ungünstige klimatische Bedingungen	mittel	hoch	mittel	Die Auswirkungen wären lokal begrenzt.
G 0.3 Wasser	k.A.	hoch	mittel	Die Auswirkungen des Vorfalls wären lokal begrenzt. Es ist eine geeignete Standortwahl zu treffen bzw. es sind zusätzliche bauliche Vorkehrungen zu treffen.
G 0.4 Verschmutzung, Staub, Korrosion	mittel	gering	mittel	Die Auswirkungen wären lokal begrenzt. Sinngemäße Umsetzung von Basis- und Standardgrundschutzanforderungen reicht aus.
G 0.5 Naturkatastrophen	gering	hoch	mittel	Die Auswirkungen der Naturkatastrophen können Komponenten in einem bestimmten Gebiet umfassen. Es ist eine geeignete Standortwahl zu treffen bzw. es sind zusätzliche bauliche Vorkehrungen zu treffen.
G 0.6 Katastrophen im Umfeld	k.A.	hoch	mittel	Die Auswirkungen wären lokal begrenzt. Es ist eine geeignete Standortwahl zu treffen.
G 0.7 Großereignisse im Umfeld	k.A.	gering	gering	Auswirkungen wären lokal begrenzt.
G 0.8 Ausfall oder Störung der Stromversorgung	mittel	hoch	mittel	Die Auswirkungen des Vorfalls wären lokal begrenzt. Die sinngemäße Umsetzung von Basis- und Standardgrundschutzanforderungen zur Stromversorgung reicht aus.
G 0.34 Anschlag	gering	hoch	mittel	Die Auswirkungen des Angriffs wären lokal begrenzt. Die sinngemäße Um-

Elementare Gefährdung	Eintritt	Schaden	Risiko	Bemerkung
				setzung von Basis- und Standard-grundschutzanforderungen zum Perimeterschutz reicht aus.
G 0.41 Sabotage	mittel	hoch	mittel	Bei physischer Zerstörung wären die Auswirkungen lokal begrenzt. Für logische Manipulation an Systemen wäre unbefugtes Eindringen und Zugang zu den Systemen die Voraussetzung.
G 0.44 Unbefugtes Eindringen in Räumlichkeiten	mittel	hoch	untragbar	Es wird auch unbefugtes Eindringen in ein Gelände betrachtet. Nach unbefugtem Eindringen kann versucht werden Komponenten zu zerstören oder in Systeme / Netze einzudringen und Funktionen und Daten zu manipulieren.

Tabelle 31: Bewertung elementare Gefährdung zu „Betriebsgelände DER-Anlage“ und „Aufstellungsort Prosumer-DER-Anlage2“ (ohne Bausteinzuordnung) 5. Risikobereich VPP

Für INF-Pros-1 Zählerkasten zur Prosumer-DER-Anlage werden nachfolgend die elementaren Gefährdungen zum Baustein INF.5 Raum oder Schrank für technische Infrastruktur (2018 CD, siehe auch Kap. 8.2.1.2) bezüglich des Risikobereiches „Vorsätzliche Überwindung oder zufällige Schäden (einschließlich höherer Gewalt) bei Infrastruktureinrichtungen der dezentralen Erzeuger bzw. Verbraucher“ bewertet.

Elementare Gefährdung	Eintritt	Schaden	Risiko	Bemerkung
G 0.01 Feuer	gering	gering	tragbar	Die Bewertung setzt voraus, dass die Grundschutzanforderungen des Bausteins erfüllt sind. Tritt das Schadensereignis ein, wären die Folgen meist lokal begrenzt.
G 0.02 Ungünstige klimatische Bedingungen	gering	gering	tragbar	
G 0.03 Wasser	gering	gering	tragbar	
G 0.04 Verschmutzung, Staub, Korrosion	gering	gering	tragbar	
G 0.05 Naturkatastrophen	gering	gering	tragbar	
G 0.08 Ausfall oder Störung der Stromversorgung	gering	gering	tragbar	
G 0.10 Ausfall oder Störung von Versorgungsnetzen	gering	gering	tragbar	
G 0.11 Ausfall oder Störung von Dienstleistern	gering	gering	tragbar	
G 0.13 Abfangen kompromittierender Strahlung	gering	gering	tragbar	Der erforderliche Aufwand scheint in einem schlechten Verhältnis zum böswilligen Effekt zu stehen
G 0.18 Fehlplanung oder fehlende Anpassung	gering	gering	tragbar	Die Bewertung setzt voraus, dass die Grundschutzanforderungen des Bausteins erfüllt sind. Tritt das Schadensereignis ein, wären die Folgen meist lokal begrenzt.
G 0.24 Zerstörung von Geräten oder Datenträgern	gering	gering	tragbar	
G 0.25 Ausfall von Geräten oder Systemen	gering	gering	tragbar	
G 0.26 Fehlfunktion von Geräten oder Systemen	gering	gering	tragbar	
G 0.29 Verstoß gegen Gesetze oder Regelungen	-	-	-	-
G 0.33 Personalausfall	-	-	-	-

Elementare Gefährdung	Eintritt	Schaden	Risiko	Bemerkung
G 0.41 Sabotage	gering	hoch	mittel	Bei physischer Zerstörung wären die Auswirkungen lokal begrenzt. Für logische Manipulation an Systemen wäre unbefugtes Eindringen und Zugang zu den Systemen die Voraussetzung.
G 0.44 Unbefugtes Eindringen in Räumlichkeiten	mittel	hoch	mittel	Unbefugtes Eindringen bzw. öffnen könnte erster Schritt in einem Spionage / Sabotage Angriff sein.

Tabelle 32: Bewertung der elementaren Gefährdung zu INF.5 Raum oder Schrank für technische Infrastruktur (CD) für den 5. Risikobereich VPP

Betrachtung im Zusammenhang

Im Folgenden werden elementare Gefährdungen, denen mit der Erfüllung von Grundschutzanforderungen adäquat begegnet werden kann nicht aufgeführt (siehe Tabelle 31).

	Wirkung auf		
Elementare Gefährdung	INF-DER-1 Betriebsgelände DER-Anlage“	INF-Pros-2 Aufstellungsort Prosumer-DER-Anlage	INF-Pros-1 Zählerkasten zur Prosumer-DER-Anlage
G 0.41 Sabotage			x
G 0.44 Unbefugtes Eindringen in Räumlichkeiten	x	x	x

Tabelle 33: Alle als relevant (über ITGS-Anforderungen hinaus) bewerteten elementaren Gefährdungen für den 5. Risikobereich VPP

Risiken:

Angriff	Bewertung vorausges. ITGS-Anf. sind umgesetzt	Zusätzliche Maßnahme(n)
Ein Angreifer kann den Perimeterschutz des Betriebsgeländes bzw. den Schutz des Aufstellungsortes der DER-Anlage überwinden.	Bis auf den Fall, dass ein Angriff fortgeführt wird und physischer Zugang / Zugriff zum Zählerkasten der Prosumer-DER-Anlage möglich ist, ist die Umsetzung der Grundschutzmaßnahmen ausreichend.	Perimeterschutz
Der Angreifer überwindet den Perimeterschutz sowie den physischen Zugangs- / Zugriffschutz des Zählerkastens und kann auf die darin verbauten Systeme (z. B. Gateway) zugreifen.	mittleres Risiko	Gateways und sonstige kritische Systeme einer Anlage müssen in einem sicheren Schrank / Raum verbaut sein (z. B. striktes Zutrittskonzept, Alarm bei Öffnung, Sicherheitsschloss).

Tabelle 34: Risiken für den 3. Risikobereich VPP

8.3 Schlussfolgerungen aus den Ergebnissen der Schwachstellen-, Bedrohungs- und Risikoanalyse

In den beiden Risikobereichen zum „Verlust von Vertraulichkeit (Schwerpunkt), Integrität und Authentizität (besonderer) personenbezogener Daten“ wird durch die Erfüllung der Grundschutzanforderungen zusammen mit der Berücksichtigung der TR 03109 eine weitreichende Absicherung erreicht. Zusätzlich ist sicherzustellen, dass die kryptografische Absicherung keine Lücken aufweist und keine Gefahr von Innentätern ausgeht.
In den beiden Risikobereichen zum „Verlust der Integrität (Schwerpunkt), Authentizität und Verfügbarkeit von Kontroll- und Steuerungsdaten und -funktionen“ wird durch die Erfüllung der Grundschutzanforderungen zusammen mit der Berücksichtigung der TR 03109 eine weitreichende Absicherung erreicht. Zusätzlich sollte berücksichtigt werden, dass die Firewall der Leitwarte als zentrale Sicherheitsinfrastruktur eine hohe Verfügbarkeit garantieren sollte. Außerdem sollte durch starke Schutzmechanismen innerhalb der dezentralen Einrichtungen die Integrität von Steuerbefehlen sichergestellt werden. Der Zugang zum Gateway darf nur nach Authentisierung mit starken Verfahren möglich sein. Es darf kein Zugang über Hintertüren möglich sein. Sicherheitsrelevante Patches müssen zeitnah eingespielt werden. Ebenso muss es möglich sein, dass auf höherwertige Verfahren, bzw. längerer Schlüssel, migriert werden kann. Für den Bereich Smart Meter Gateway gelten diesbezüglich bereits strenge Anforderungen (TR 03109). Entsprechendes sollte bei allen Arten von Gateways umgesetzt werden.
Im Risikobereich „Vorsätzliche Überwindung oder zufällige Schäden (einschließlich höherer Gewalt) bei Infrastruktureinrichtungen der dezentralen Erzeuger bzw. Verbraucher“ sind für Betriebsgelände oder allgemeine Aufstellungsorte keine Bausteine vorhanden. Es sollten Maßnahmen zur Zutrittskontrolle und zum Schutz vor höherer Gewalt umgesetzt werden, wobei das Risiko der physischen Beeinträchtigung der Anlagen als begrenzt eingeschätzt werden kann, da es sich im Schadensfall um lokale Vorfälle handelt. Das größte Risiko in diesem Bereich besteht, wenn sowohl Perimeterschutz als auch der Schutz des Einbauortes (Schrank, Kasten, kleiner Raum) der Gateways und weiterer Geräte, zu schwach ist und es einem Angreifer gelingt physisch auf die Geräte zuzugreifen.

9 Alternativer Ansatz Risikobehandlung: Direkte Zuordnung von Anforderungen aus anderen Standards

Ein bestimmtes Maß an Restrisiko verbleibt selbst bei vollständiger Erfüllung aller Anforderungen. Gerade durch die lückenhafte Modellierungsmöglichkeit der Smart-Grid-Zielobjekte durch Bausteine des IT-Grundschutzkompendiums ist das Restrisiko in diesem Grundschutzprofil in der aktuellen Version besonders groß.
Für die Zielobjektkategorien Netze und Kommunikation, IT-Systeme und industrielle IT werden daher weitere Anforderungen definiert, welche aus der **IEC 62351** mit dem Titel „*Power systems management and associated information exchange - Data and communications security”* und der **IEC 62442-3-3** mit dem Titel „*Industrial communication networks – Network and system security - System security requirements and security levels“* entnommen werden konnten. Somit wird ein Teil des verbleibenden Restrisikos abgesichert.

	Netze und Kommunikation:	via AMI Backhaul Network	Home & Building Integration Bus	DER Integration Bus	Intra-center Integration BUS	Operator Backhaul Network	via Backbone Network	Direct wire connection	IT-Systeme:	DER SCADA System	Energy Management System	Forecasting System for the Gener-	EMS User Interface	Industrielle IT:	DER Gateway	Device Energy Management	DER Equipment 1	DER Equipment 2	External Smart Meter Gateway	Internal Smart Meter Gateway
IEC 62351 - Power systems management and associated information exchange - Data and communications security																				
IEC 62351-3 — Security for any profiles including TCP/IP		x		x	x	x				x					x					x
IEC 62351-4 — Security for any profiles including MMS		x		x	x	x				x					x					x
IEC 62351-5 — Security for any profiles including IEC 60870-5		x		x	x	x				x					x					x
IEC 62351-6 — Security for IEC 61850 profiles		x		x	x	x				x					x					x
IEC 62351-7 — Security through network and system management		x		x	x	x	x			x	x	x	x		x	x				x
IEC 62351-8 — Role-based access control										x	x	x	x		x	x				x
IEC 62351-9 — Key Management										x						x				x
IEC 62351-10 — Security Architecture				x		x				x	x	x	x		x	x				x
IEC 62443-3-3 - System security requirements and security levels																				
FR 1 - Identification and authentication control																				
SR 1.1 - Human user identification and authentication										x			x			x				
SR 1.2 - Software process and device identification and authentication										x	x	x	x		x	x				x
SR 1.3 - Account management										x	x	x				x				
SR 1.4 - Identifier management										x	x	x				x				
SR 1.5 - Authenticator management										x	x	x				x				
SR 1.6 - Wireless access management													x							

SR 1.7 - Strength of password-based authentication									x			x			x			
SR 1.8 - Public key infrastructure (PKI) certificates									x					x	x			x
SR 1.9 - Strength of public key authentication									x					x	x			x
SR 1.10 - Authenticator feedback									x	x	x	x			x			
SR 1.11 - Unsuccessful login attempts									x	x	x	x			x			
SR 1.12 - System use notification																		
SR 1.13 - Access via untrusted networks									x						x			
FR 2 - Use control																		
SR 2.1 - Authorization enforcement									x	x	x	x			x			
SR 2.2 - Wireless use control												x						
SR 2.3 - Use control for portable and mobile devices									x	x	x	x			x			
SR 2.4 - Mobile code												x						
SR 2.5 - Session lock												x						
SR 2.6 - Remote session termination									x	x	x	x			x			
SR 2.7 - Concurrent session control									x	x	x	x			x			
SR 2.8 - Auditable events									x	x	x	x			x			
SR 2.9 - Audit storage capacity									x	x	x	x			x			
SR 2.10 - Response to audit processing failures									x	x	x	x			x			
SR 2.11 - Timestamps									x	x	x	x		x	x			x
SR 2.12 - Non-repudiation									x	x	x	x			x			
FR 3 - System integrity																		
SR 3.1 - Communication integrity			x	x	x			x	x	x	x	x		x	x	x	x	x
SR 3.2 - Malicious code protection									x	x	x	x		x	x			x
SR 3.3 - Security functionality verification									x	x	x	x		x	x			x
SR 3.4 - Software and information integrity									x	x	x	x		x	x			x
SR 3.5 - Input validation			x	x	x			x	x	x	x	x		x	x			x
SR 3.6 - Deterministic output									x			x		x	x	x	x	x
SR 3.7 - Error handling			x	x	x			x	x	x	x	x		x	x			x
SR 3.8 - Session integrity									x	x	x	x		x	x			x
SR 3.9 - Protection of audit information									x	x	x	x		x	x			x

FR 4 - Data confidentiality																		
SR 4.1 - Information confidentiality									x	x	x	x		x	x			x
SR 4.2 - Information persistence									x	x	x	x			x			
SR 4.3 - Use of cryptography									x	x	x	x		x	x			x
FR 5 - Restricted data flow																		
SR 5.1 - Network segmentation			x	x	x				x			x		x				x
SR 5.2 - Zone boundary protection			x	x	x				x			x		x				x
SR 5.3 - General purpose person-to-person communication restrictions			x	x	x				x	x	x	x						
SR 5.4 - Application partitioning									x	x	x							
FR 6 - Timely response to events																		
SR 6.1 - Audit log accessibility									x	x	x	x		x	x			x
SR 6.2 - Continuous monitoring									x	x	x	x		x	x			x
FR 7 - Resource availability																		
SR 7.1 - Denial of service protection									x	x		x		x	x			x
SR 7.2 - Resource management									x						x			
SR 7.3 - Control system backup									x	x	x	x		x	x			x
SR 7.4 - Control system recovery and reconstitution									x	x	x	x		x	x			x
SR 7.5 - Emergency power									x	x	x	x		x	x			x
SR 7.6 - Network and security configuration settings									x	x	x	x		x	x	x	x	x
SR 7.7 - Least functionality									x	x	x	x		x	x			x
SR 7.8 - Control system component inventory									x	x	x	x			x			

10 Anwendungshinweise

Die ermittelten Anforderungen sind in das Gesamtsicherheitskonzept eines virtuellen Kraftwerks zu integrieren und im Zuge der Realisierungsplanung umzusetzen.

11 Unterstützende Informationen

Detaillierte Informationen zu den einzelnen Anforderungen finden sich in den Umsetzungshinweisen der einzelnen Bausteine des IT-Grundschutzes sowie in den Anforderungsbeschreibungen der IEC 62351 und IEC 62443.

12 Abkürzungsverzeichnis

AMI	Automated Metering Infrastructure
BSI	Bundesamt für Sicherheit in der Informationstechnik
CEM	Customer Energy Management
DER	Decentralized Energy Resource
DMS	Distribution Management System
EDMS	Energy Data Management System
EMS	Energy Management System
IEC	International Electrotechnical Commission
IKT	Informations- und Kommunikationstechnik
ISMS	Information Security Management System
ISO	International Organization for Standardization
IT	Informationstechnik
PDCA	Plan-Do-Check-Act
SCADA	Supervisory Control and Data Acquisition
SGAM	Smart Grid Architecture Model
SL	Security Level
VPP	Virtual Power Plant

Anhang: Exemplarische Geschäftsprozesslandkarte für ein IT-Grundschutz-Profil eines virtuellen Kraftwerks

Nachfolgend ist das Ergebnis, so wie in modernen Grundschutzprofilen üblich, in Form von „Landkarten“ für (exemplarische einen) der behandelten Geschäftsprozesse zusammengefasst dargestellt.

In einer „Landkarte“ werden in Spalte 1 die relevanten Geschäftsprozesse benannt. In Spalte 2 werden die Geschäftsprozesse anhand von typischen Aufgaben in diesem Bereich näher beschrieben. Daraus ergeben sich Anwendungen, die für die Erfüllung der Aufgaben benötigt werden (Spalte 3). Diese Anwendungen laufen auf entsprechenden IT-Systemen (Spalte 4), die sich in bestimmten Räumlichkeiten des Betriebes befinden (Spalte 5).

Die hier dargestellte Landkarte beschränkt sich auf einen Geschäftsprozess. Die angegebene Modellierung ist zum Teil exemplarisch zu sehen, da sie im Produktivbetrieb von den tatsächlich eingesetzten Hard- und Softwareprodukten abhängt.

Ergebnisdokument AS 12.2.1

„Gesetze, Regularien, Richtlinien, Compliance, Zertifizierungen“

Autoren:

Christian Bruns (BTC AG), Christine Rosinger (OFFIS, AS12.2.1-Verantwortliche), Konrad Rosmus (IABG), Rolf Strenge (EWE-Netz)

20.09.2017

Gefördert durch:

Bundesministerium für Wirtschaft und Energie

aufgrund eines Beschlusses des Deutschen Bundestages

Historie des Dokuments

Version	Datum	Name	Änderungen	Dateiname
-	24.02.2017	Christine Rosinger, OFFIS	Datei erstellt, 1. Vorschlag für grobe Gliederung.	2017-02-27_AS12.2.1_Gesetze, Regularien, Richtlinien, Compliance, Zertifizierungen.docx
-	15.03.2017	Christine Rosinger, OFFIS	Verantwortlichkeiten in Abschnitt 3 ergänzt.	2017-03-15_AS12.2.1_Gesetze, Regularien, Richtlinien, Compliance, Zertifizierungen.docx
-	22.03.2017	Rolf Strenge, EWE NETZ	Ergänzung 3.1.1 – 3.1.4, Umsortierung der Abschnitte	2017-03-22_AS12.2.1_Gesetze Regularien Richtlinien Compliance Zertifizierungen_RolfStrenge.docx
-	26.04.2017	Christian Bruns, BTC AG	Abschnitt 2.3 eingefügt.	2017-03-15_AS12.2.1_Gesetze, Regularien, Richtlinien, Compliance, Zertifizierungen – CBr.docx
-	02.05.2017	Konrad Rosmus, IABG	Abschnitte 2.2.1, 2.2.2, 2.2.9 – 2.2.12 eingefügt.	2017-05-02_AS12.2.1_Gesetze Regularien Richtlinien Compliance Zertifizierungen_Konrad.docx
-	04.05.2017	Christine Rosinger, OFFIS	Fehlende Abschnitte und Zusammenfassungen hinzugefügt, erstes Kontrolllesen.	2017-05-04_AS12.2.1_Gesetze, Regularien, Richtlinien, Compliance, Zertifizierungen.docx
-	17.05.2017	Christine Rosinger, OFFIS	Überarbeitungen aus Telko eingebaut.	2017-05-17_AS12.2.1_Gesetze, Regularien, Richtlinien, Compliance, Zertifizierungen.docx
-	19.05.2017	Rolf Strenge, EWE NETZ	Ergänzung zu IT-Sicherheitsgesetz	2017-05-19_AS12.2.1_Gesetze Regularien Richtlinien Compliance Zertifizierungen.docx
-	24.05.2017	Christine Rosinger, OFFIS	Änderungen angenommen.	2017-05-24_AS12.2.1_Gesetze, Regularien, Richtlinien, Compliance, Zertifizierungen.docx
-	08.06.2017	Christine Rosinger, OFFIS	Kleine Ergänzungen in Abschnitt 2.3	2017-06-08_AS12.2.1_Gesetze, Regularien, Richtlinien, Compliance, Zertifizierungen.docx

-	10.06.2017	Christian Bruns, BTC	Ergänzungen zu BSI-Grundschutzbausteinen in 2.3	2017-06-10_AS12.2.1_Gesetze, Regularien, Richtlinien, Compliance, Zertifizierungen.docx
-	12.06.2017	Christine Rosinger, OFFIS	Überarbeitungen aus Telko hinzugefügt.	2017-06-12_AS12.2.1_Gesetze, Regularien, Richtlinien, Compliance, Zertifizierungen.docx
-	13.06.2017	Konrad Rosmus, IABG	Ergänzung Kap. 2.4 Zertifizierung; Inhaltsverzeichnis	20170613_AS12.2.1_Gesetze, Regularien, Richtlinien, Compliance, Zertifizierungen.docx
-	14.06.2017	Christine Rosinger, OFFIS	Ergänzungen in den Abschnitten 2.3.5, 2.4 und 3	2017-06-14_AS12.2.1_Gesetze, Regularien, Richtlinien, Compliance, Zertifizierungen.docx
-	20.06.2017	Christine Rosinger, OFFIS	Dokument finalisiert und an AP12 Verteiler geschickt.	2017-06-20_AS12.2.1_Gesetze, Regularien, Richtlinien, Compliance, Zertifizierungen.docx
1.0	06.07.2017	Christine Rosinger, OFFIS	Erhaltene Kommentare eingearbeitet, finalisiert. Damit ist AS12.2.1 abgeschlossen. Weitere Bearbeitung dieses Dokuments erfolgt in AS12.2.4.	2017-07-06_AS12.2.1_Gesetze, Regularien, Richtlinien, Compliance, Zertifizierungen_V1.0.docx
1.01	01.08.2017	Christine Rosinger, OFFIS	Rückmeldung von AP2 (Christian Bruns) eingepflegt.	2017-08-01_AS12.2.1_Gesetze, Regularien, Richtlinien, Compliance, Zertifizierungen_V1.01.docx
1.02	11.08.2017	Christine Rosinger, OFFIS	Rückmeldung von AP6 (Steffen Hofer) eingepflegt.	2017-08-11_AS12.2.1_Gesetze, Regularien, Richtlinien, Compliance, Zertifizierungen_V1.02.docx
1.03	20.09.2017	Fabian Karl, PPC	Abschnitt 2.4.5 eingefügt	2017-09-20_AS12.2.1_Gesetze, Regularien, Richtlinien, Compliance, Zertifizierungen_V1.03.docx
2.0	09.12.2020	Christine Rosinger, OFFIS	Dokument auf Version 2.0 gesetzt	2020-12-09_AS12.2.1_Gesetze, Regularien, Richtlinien, Compliance, Zertifizierungen_V2.0.docx

Inhalt

Abkürzungsverzeichnis 6
1 Einordnung, Ziele und Gliederung 8
2 Kurzbeschreibung der identifizierten Regularien 8
2.1 Gesetze und Verordnungen 9
2.1.1 IT-Sicherheitsgesetz 9
2.1.2 BSI-Gesetz 9
2.1.3 EU NIS-Richtlinie 10
2.1.4 Energiewirtschaftsgesetz (EnWG) 10
2.1.5 IT-Sicherheitskatalog der Bundesnetzagentur 11
2.1.6 Messstellenbetriebsgesetz (MsbG) 11
2.1.7 Datenschutzgesetze 11
2.1.8 EEG 13
2.1.9 KWKG 13
2.1.10 Zusammenfassung „Gesetze und Verordnungen“ 13
2.2 Normen, Standards und Richtlinien 15
2.2.1 ISO/IEC 27000-Reihe 15
2.2.2 BSI Grundschutz 20
2.2.3 BDEW Whitepaper 27
2.2.4 IEC 62351 27
2.2.5 IEC 62443 29
2.2.6 NISTIR 7628 30
2.2.7 NERC CIP 30
2.2.8 ENISA: Appropriate security measures for smart grids 30
2.2.9 BSI TR-03109 31
2.2.10 BSI TR-03116-3 33
2.2.11 BSI TR-03145 34
2.2.12 Common Criteria (ISO/IEC 15408) 35
2.2.13 Zusammenfassung „Normen, Standards und Richtlinien“ 36
2.3 Informationssicherheit in der Software Entwicklung 38
2.3.1 Klassische Verfahren Softwareentwicklung 39
2.3.2 Agile Verfahren Softwareentwicklung 40
2.3.3 Security-by-Design Prinzipien und Security Patterns 41

2.3.4 Best Practices für Software(entwicklung) 44
2.3.5 Anforderungen an Softwareentwicklung gemäß BSI 45
2.3.6 Zusammenfassung „Software Security“ 47
2.4 Zertifizierungen 47
2.4.1 DIN ISO/IEC 27001 48
2.4.2 ISO 27001 auf Basis IT-Grundschutz 48
2.4.3 IT-Sicherheitskatalog 50
2.4.4 Smart Meter Gateway Administrator 52
2.4.5 Secure CA Operations 54
2.4.6 Zusammenfassung „Zertifizierungen“ 54
3 Zusammenfassung 55
4 Abbildungsverzeichnis 57
5 Tabellenverzeichnis 57

Abkürzungsverzeichnis

Abkürzung	Bedeutung
AP	Arbeitspaket
AS	Arbeitsschritt
ASD	Adaptive Software Development
BDEW	Bundesverband der Energie- und Wasserwirtschaft e.V.
BDSG	Bundesdatenschutzgesetz
BMWi	Bundesministerium für Wirtschaft und Energie
BNetzA	Bundesnetzagentur
BSI	Bundesamt für Sicherheit in der Informationstechnik
CA	Certification Authority
CC	Common Criteria
CEM	Common Methodology for Information Technology Security Evaluation
CIP	Critical Infrastructure Protection
CP	Certificate Policy
CPU	Central Processing Unit
DACH	Deutschland, Österreich und die Schweiz
DAkkS	Deutsche Akkreditierungsstelle
DIN	Deutsches Institut für Normung e. V.
DSAnpUG-EU	Datenschutz-Anpassungs- und -Umsetzungsgesetz EU
EAL	Evaluation Assurance Level
EDV	Elektronische Datenverarbeitung
EEG	Erneuerbare-Energien-Gesetz
ENISA	Europäische Agentur für Netz- und Informationssicherheit
ENISA	European Network and Information Security Agency
EnWG	Energiewirtschaftsgesetz
EU	Europäische Union
EU-DSGV	EU Datenschutzgrundverordnung
EVG	Evaluationsgegenstand
FDD	Feature-Driven Development
HAN	Home Area Network
I&A	Identification and Authentication
ICS	Industrial Control Systems
IEC	International Electrotechnical Commission, deutsch: Internationale Elektrotechnische Kommission
IoT	Internet-of-Things
ISB	Informationssicherheitsbeauftragter
ISMS	Informationssicherheitsmanagementsystem

Abkürzung	Bedeutung
ISO	International Organization for Standardization, deutsch: Internationale Organisation für Normung
IT-SiBe	IT-Sicherheitsbeauftragter
KRITIS	Kritische Infrastrukturen
KWKG	Kraft-Wärme-Kopplungsgesetz
LMN	Local Metrological Network
MsbG	Messstellenbetriebsgesetz
NDSG	Niedersächsisches Datenschutzgesetz
NERC	North American Electric Reliability Corporation
NIS	Netz- und Informationssicherheit
NIST	National Institute of Standards and Technology
NISTIR	NIST Internal/Interagency Report
OWASP	Open Web Application Security Project
PACE	Password Authenticated Connection Establishment
PDCA	Plan-Do-Check-Act
PKI	Public Key Infrastructure
RBAC	Role Based Access Control
SIA	Seamless Integration Architecture
SINTEG	Schaufenster intelligente Energie - Digitale Agenda für die Energiewende
SMGW	Smart Meter Gateway
SM-PKI	Smart Metering - Public Key Infrastruktur
SQL	Structured Query Language
TAP	Teilarbeitspaket
TC	Trust Center
TK	Telekommunikation
TKG	Telekommunikationsgesetz
TLS	Transport Layer Security
TMG	Telemediengesetz
TR	Technische Richtlinie
TÜV	Technischer Überwachungsverein
UML	Unified Modeling Language
WAN	Wide Area Network
XP	Xtreme Programming

Ergebnisdokument AS 12.2.1

„Gesetze, Regularien, Richtlinien, Compliance, Zertifizierungen“

1 Einordnung, Ziele und Gliederung

Enera ist eins der fünf durch das Bundesministeriums für Wirtschaft und Energie (BMWi) geförderten Projekte des Förderprogramms „Schaufenster intelligente Energie – Digitale Agenda für die Energiewende“ (SINTEG)[1]. Im Projekt werden Lösungen zu den drei Themenschwerpunkten Netz, Markt und Daten in der Modellregion im Nordwesten Niedersachsens entwickelt und erprobt. Das **Arbeitspaket (AP) 12** innerhalb dieses Projekts beschäftigt sich mit der informationstechnischen Entwicklung der enera Gesamtarchitektur inklusive eines Informationssicherheitskonzepts.

Das **Teilarbeitspaket (TAP) 12.2** befasst sich mit dem Informationssicherheitskonzept. Der dazugehörige **Arbeitsschritt (AS) 12.2.1** mit dem Titel „Gesetze, Regularien, Richtlinien, Compliance, Zertifizierungen“ setzt sich innerhalb dieses TAPs damit auseinander, welche nationalen und internationalen Regularien, also Gesetze, Richtlinien, Verordnungen, Normen und Standards in Bezug auf Informationssicherheit für das Projekt relevant sind. Weiterhin werden Empfehlungen gegeben, wie diese Vorschriften sinnvoll und regelkonform im Projekt eingesetzt werden können (Compliance). Zusätzlich werden vorgeschriebene Zertifizierungen in Bezug auf Informationssicherheit betrachtet. Insgesamt ist es in diesem AS also das Ziel, die Landschaft der Regularien in Bezug auf Informationssicherheit für dieses Projekt zu beleuchten und entsprechende Empfehlungen daraus für enera abzuleiten. Die Ergebnisse dieses Arbeitsschritts werden innerhalb dieses Dokuments festgehalten.

Das weitere Dokument gliedert sich wie folgt: Nachfolgend gibt Abschnitt 2 einen Überblick zu Regularien in Bezug auf Informationssicherheit, die für das Projekt enera relevant sein können. Die Relevanz für die einzelnen Arbeitspakete von enera wird außerdem beleuchtet. Abschließend gibt Abschnitt 3 eine Kurzzusammenfassung.

2 Kurzbeschreibung der identifizierten Regularien

In diesem Abschnitt werden relevante Regularien für Informationssicherheit kurz beschrieben und deren Bedeutsamkeit für das Projekt enera erläutert. Es wurden dabei die Regularien betrachtet, die einen Beitrag im Projektkontext von enera liefern. Weitere Entwicklungen für Regularien für Informationssicherheit werden im Kontext von AS 12.2.4 „Governance, Compliance und Datenschutz: Erhebungen, Strukturen und Management“ überwacht und bei Bedarf überarbeitet.

Innerhalb von Abschnitt 2 werden zunächst in Abschnitt 2.1 Gesetze und Verordnungen beleuchtet, Abschnitt 2.2 gibt einen Überblick zu Normen, Standards und Richtlinien, ab-

[1] Siehe auch die Seite des SINTEG-Förderprogramms auf der Homepage des BMWi https://www.bmwi.de/Redaktion/DE/Artikel/Energie/sinteg.html.

schließend werden in Abschnitt 2.3 entsprechende Richtlinien zu Software Security beschrieben. Jeder dieser drei Abschnitte wird mit einer Zusammenfassung abgeschlossen, in der die Regularien übersichtlich dargestellt werden, sowie der Zusammenhang zum Projekt enera erläutert wird.

2.1 Gesetze und Verordnungen

Dieser Abschnitt gibt eine Kurzbeschreibung verschiedener im Kontext von Informationssicherheit relevanter Gesetze, Verordnungen und gesetzlicher Richtlinien. Dabei werden sowohl nationale als auch internationale Regularien beleuchtet.

2.1.1 IT-Sicherheitsgesetz[2]

Das IT-Sicherheitsgesetz (Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme) ist ein am 25.07.2015 in Kraft getretenes Gesetz zur Verbesserung des Schutzes der Informationssicherheit von besonders gefährdeten Infrastrukturen (sogenannten kritischen Infrastrukturen, KRITIS) wie Energie, Wasser, Gesundheit oder Telekommunikation.
Das Gesetz ist ein Artikelgesetz, welches Änderungen in verschiedenen anderen Gesetzen bewirkt hat, darunter das BSI-Gesetz, das Energiewirtschaftsgesetz (EnWG), das Telemediengesetz (TMG) und das Telekommunikationsgesetz (TKG).
Um zu ermitteln, welche Unternehmen zu den kritischen Infrastrukturen zählen, für die diese Anforderungen gelten, ist die Verordnung zur Bestimmung Kritischer Infrastrukturen (BSI-Kritisverordnung - BSI-KritisV)[3] gemäß § 10 Absatz 1 des BSI[4]-Gesetzes in Kraft getreten.
Die dort definierten Schwellwerte geben den Wert vor, bei dessen Erreichen oder dessen Überschreitung der Versorgungsgrad einer Anlage oder Teilen davon als bedeutend im Sinne von § 10 Absatz 1 Satz 1 des BSI-Gesetzes anzusehen ist. Diese Schwellwerte sind in Energiemengen ausgedrückt und leiten sich jeweils aus dem Durchschnittsverbrauch von 500.000 Personen ab.

2.1.2 BSI-Gesetz[5]

Das „BSI-Gesetz“ ist das Gesetz, das die Aufgaben und Befugnisse des Bundesamts für Sicherheit in der Informationstechnik (BSI) festlegt.
Besondere Relevanz hat das BSI-Gesetz dadurch bekommen, dass durch das IT-Sicherheitsgesetz Änderungen in Bezug auf die kritischen Infrastrukturen (KRITIS) eingeflossen sind.
Die wesentlichen Änderungen diesbezüglich sind:

- Betreiber Kritischer Infrastrukturen müssen gemäß § 8a die Einhaltung von IT-Sicherheit nach dem Stand der Technik gegenüber dem BSI nachweisen. Das BSI darf im Einvernehmen mit den Aufsichtsbehörden die Beseitigung von Sicherheitsmängeln anordnen.

---

[2] Informationen des BSI zum IT-Sicherheitsgesetz können unter https://www.bsi.bund.de/DE/Themen/Industrie_KRITIS/IT-SiG/it_sig_node.html abgerufen werden.
[3] Die BSI-KritisV kann unter https://www.gesetze-im-internet.de/bundesrecht/bsi-kritisv/gesamt.pdf abgerufen werden.
[4] BSI steht für Bundesamt für Sicherheit in der Informationstechnik.
[5] Der Text des BSI-Gesetzes kann unter https://www.gesetze-im-internet.de/bsig_2009/ abgerufen werden.

- Das BSI ist gemäß § 8b die zentrale Meldestelle für die IT-Sicherheitsvorfälle der KRITIS Unternehmen. Diese müssen dem BSI erhebliche Störungen ihrer IT melden, sofern sie Auswirkungen auf die Verfügbarkeit kritischer Dienstleistungen haben können oder diese akut bedrohen.
- Sofern bei einem Betreiber Kritischer Infrastrukturen meldepflichtige Störungen der IT auftreten, darf das BSI auch die Hersteller der entsprechenden IT-Produkte und Systeme zur Mitwirkung verpflichten.
- Zu den Aufgaben des BSI gehört es auch IT-Produkte auf ihre Sicherheit hin zu untersuchen.

2.1.3 EU NIS-Richtlinie[6]

Die EU NIS-Richtlinie – NIS steht dabei für Netz- und Informationssicherheit – wurde parallel zur Europäischen Cybersicherheitsstrategie von der Europäischen Kommission entworfen und im Juli 2016 verabschiedet. Diese Richtlinie soll dazu dienen, die Netz- und Informationssicherheit in Europa zu verbessern und dabei private Betreiber von Netzwerk- und Informationssystemen zu verpflichten die entsprechenden Mindestanforderungen zu gewährleisten. Zusätzlich muss ein Berichtssystem zwischen den einzelnen Mitgliedsstaaten untereinander und mit der ENISA[7] (Europäische Agentur für Netz und Informationssicherheit) etabliert werden. Bis Mai 2018 muss die Richtlinie durch gesetzliche Anpassung ins deutsche Recht übernommen werden. Die Richtlinie entspricht allerdings in vielen Punkten dem deutschen IT-Sicherheitsgesetz und es muss nur eine Mindestharmonisierung erfolgen, das heißt, es müssen nur Anpassungen erfolgen, wo das Mindestschutzniveau der Richtlinie unterschritten wird. Relevant ist diese Richtlinie für „Betreiber wesentlicher Dienste und Anbieter digitaler Dienste“ und ist somit relevant für das Projekt enera.

2.1.4 Energiewirtschaftsgesetz (EnWG)

Der § 11 des EnWG wurde ebenfalls durch das IT-Sicherheitsgesetz geändert. Hier werden Anforderungen an die IT-Sicherheit an Netz- und Anlagenbetreiber gestellt, die teilweise Ausnahmen zu den Vorgaben aus dem geänderten BSI-Gesetz darstellen. Unter anderem wird den Netzbetreibern die Einhaltung des sogenannten IT-Sicherheitskatalogs der Bundesnetzagentur auferlegt.
Weiterhin wird in § 14a für steuerbare Verbrauchseinrichtungen in der Niederspannung vorgeschrieben, die Anforderungen des Messstellenbetriebsgesetzes (siehe Abschnitt 2.1.6) zu berücksichtigen.

[6] Die EU NIS Richtlinie kann unter http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016L1148&from=DE abgerufen werden.
[7] Siehe https://www.enisa.europa.eu/.

2.1.5 IT-Sicherheitskatalog[8] der Bundesnetzagentur

Der IT-Sicherheitskatalog gemäß §11 Absatz 1a Energiewirtschaftsgesetz der Bundesnetzagentur (BNetzA) verpflichtet Strom- und Gasnetzbetreiber zur Einhaltung von konkreten Vorgaben in Bezug auf Informationssicherheit. Dazu zählen im Wesentlichen die Einführung und der Betrieb eines Informationssicherheitsmanagementsystems (ISMS) gemäß DIN ISO/IEC 27001 unter Berücksichtigung der ergänzenden Normen DIN ISO/IEC 27002 und DIN ISO/IEC 27019. Spätestens bis zum 31. Januar 2018 muss die Erfüllung dieser Anforderungen durch die Vorlage eines von einer akkreditierten Zertifizierungsstelle ausgestellten Zertifikats nachgewiesen werden.
Die Vorgaben an die Zertifizierungsstellen für diese Zertifizierung werden in einem eigenen Konformitätsbewertungsprogramm festgelegt (Konformitätsbewertungsprogramm zur Akkreditierung von Zertifizierungsstellen für den IT-Sicherheitskatalog gemäß § 11 Absatz 1a Energiewirtschaftsgesetz auf der Grundlage der ISO/IEC 27006).

2.1.6 Messstellenbetriebsgesetz (MsbG)[9]

Das MsbG beschreibt Regelungen von Messstellen der leitungsgebundenen Energieversorgung inkl. moderner Messeinrichtungen und intelligenter Messsysteme[10], sowie der Ausgestaltung des Messbetriebs. Dabei werden technische Mindestanforderungen an den Einsatz von intelligenten Messsystemen und deren Kommunikation festgelegt. Es werden auch insbesondere die Sicherheitsanforderungen durch die Schutzprofile und Technischen Richtlinien (TR) des BSI, z.B. BSI-CC-PP-0073-2014 (Schutzprofil Smart Meter Gateway), BSI-CC-PP-0077-V2-2015 (Schutzprofil Sicherheitsmodul), BSI TR-03109 (verschiedene Technische Richtlinien), festgelegt, sowie entsprechende Zertifikatsnachweise (z.B. Zertifizierung der Gateway-Administratoren) vorgeschrieben. Außerdem werden Regelungen zur Erhebung, Verarbeitung und Nutzung personenbezogener Daten beschrieben (Datenschutz). Dieses Gesetz ist am 02.09.2016 in Kraft getreten und ist für zukünftig eingebaute intelligente Messsysteme relevant. Dabei müssen Messstellenbetreiber, wenn technisch möglich (§ 30 MsbG) und wirtschaftliche vertretbar (§ 31 MsbG), Letztverbraucher mit über 6000 Kilowattstunden pro Jahr und Anlagenbetreiber mit einer installierten Leistung über 7 Kilowatt mit intelligenten Messsystemen ausstatten. Unter diesen Grenzwerten können ebenfalls intelligente Messsysteme durch den Messstellenbetreiber eingesetzt werden, es müssen aber mindestens moderne Messeinrichtungen verwendet werden (§ 29 MsbG).

2.1.7 Datenschutzgesetze

Insgesamt gibt es Datenschutzgesetze auf verschiedenen Ebenen. In diesem Dokument werden zum einen das Niedersächsische Datenschutzgesetz (NDSG) aufgrund der Örtlich-

[8] Der Text des IT-Sicherheitskatalogs kann unter https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Energie/Unternehmen_Institutionen/Versorgungssicherheit/IT_Sicherheit/IT_Sicherheitskatalog_08-2015.pdf;jsessionid=DBAE00EEDD0E4FC2E7E1EB36C21E55AF?__blob=publicationFile&v=1 abgerufen werden.
[9] Der Text des MsbG kann unter https://www.gesetze-im-internet.de/messbg/ abgerufen werden.
[10] Die Definitionen der Begriffe „moderne Messeinrichtung“ und „intelligenten Messsystems“ sind in § 2 MsbG festgelegt.

keit der Modellregion in Abschnitt 2.1.7.1, das Bundesdatenschutzgesetz (BDSG) in Abschnitt 2.1.7.2 und die EU Datenschutzgrundverordnung (EU-DSGVO) in Abschnitt 2.1.7.3 kurz beschrieben. Bei einem Transfer in andere Modellregionen bzw. Regionen anderer Bundesländer müssen evtl. andere Landesdatenschutzgesetze berücksichtigt werden.
Innerhalb von enera im Rahmen von AS 12.2.4 mit dem Titel „Governance, Compliance und Datenschutz: Erhebungen, Strukturen und Management“ soll noch Kontakt mit der Landesbeauftragten für den Datenschutz in Niedersachsen Frau Barbara Thiel[11] aufgenommen werden, um diese Thematik zu diskutieren und abzuklären. Evtl. kann in Bezug auf Datenschutzgesetze auch juristischer Rat aus AP8 eingeholt werden. Diese Schritte werden im Rahmen von AS 12.2.4 überwacht und bearbeitet.
Da die Neuordnung des Datenschutzes in Europa aufgrund der EU-Datenschutzgrundverordnung deutlich in die Projektlaufzeit von enera fällt, muss dieser Abschnitt insgesamt nach Inkrafttreten von neuen und Wegfall alter Datenschutzgesetze nochmals überprüft werden.

2.1.7.1 Niedersächsisches Datenschutzgesetz (NDSG)[12]

Das Niedersächsische Datenschutzgesetz (NDSG) gilt für die Verarbeitung personenbezogener Daten durch Behörden und sonstige öffentliche Stellen. Ob die einzelnen Unternehmen in enera zu diesen "Behörden und sonstigen öffentlichen Stellen" zu zählen, muss noch geklärt werden. Es gibt in § 2 Abs. 3 eine Ausnahme für "öffentliche Wettbewerbsunternehmen", hier sollen dann nur die §§ 19, 21 bis 23 zur „Datenschutzkontrolle“ sowie § 8 zur „Verfahrensbeschreibung“ und § 26 zum „Fernmessen und Fernwirken“ gelten, um die Chancengleichheit im Wettbewerb zu sichern. Zu ebendiesem § 26 (Fernmessen und Fernwirken) schreibt der Datenschutzbeauftragte in seinem Kommentar[13] zum NDSG auf Seite 136, dass "für Stromlieferanten heutzutage in der Regel das BDSG Anwendung finden wird". Daher findet das NDSG in enera vermutlich keine Anwendung.

2.1.7.2 Bundesdatenschutzgesetz (BDSG)[14]

Das BDSG gilt nach § 1 Abs. 2 für "die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch" (neben öffentlichen Stellen) "3. nicht-öffentlichen Stellen, soweit sie die Daten unter Einsatz von Datenverarbeitungsanlagen verarbeiten, nutzen oder dafür erheben oder die Daten in oder aus nicht automatisierten Dateien verarbeiten, nutzen oder dafür erheben, ...". Damit ist das BDSG im Projekt enera zu berücksichtigen, so lange es nicht durch andere Gesetze ersetzt wird (wie es durch das Datenschutz-Anpassungs- und -

[11] Siehe http://www.lfd.niedersachsen.de/wir_ueber_uns/landesbeauftragte/die-landesbeauftragte-fuer-den-datenschutz-niedersachsen-130186.html.
[12] Das NDSG kann unter http://www.lfd.niedersachsen.de/download/32372/Niedersaechsisches_Datenschutzgesetz_Stand_12.12.2012_.pdf abgerufen werden.
[13] Der Kommentar des Datenschutzbeauftragten des Landes Niedersachsens ist unter http://www.lfd.niedersachsen.de/download/32433/NDSG_mit_Kommentar_Stand_November_2014_.pdf abrufbar.
[14] Der Text des BDSG kann unter https://www.gesetze-im-internet.de/bdsg_1990/ abgerufen werden.

Umsetzungsgesetz EU (DSAnpUG-EU) erfolgen soll), und Prinzipien z.B. wie Datensparsamkeit und Datenvermeidung (§ 3a) umzusetzen.

2.1.7.3 EU Datenschutzgrundverordnung (EU-DSGVO)

mDarin sollen nur sogenannte Öffnungsklauseln den einzelnen Ländern Möglichkeiten eröffnen, nationale Regelungen zu erlassen, es darf aber nicht der Datenschutz durch nationale Regelungen abgeschwächt oder verstärkt werden. In Deutschland wird die EU-DSGVO durch das Datenschutz-Anpassungs- und -Umsetzungsgesetz EU (DSAnpUG-EU) umgesetzt. Das DSAnpUG-EU soll nationales Datenschutzrecht aufheben oder demnächst unwirksame Regelungen des bisherigen BDSG in andere Gesetzesbereiche überführen, es passt Regelungen an und schafft teils neue Vorschriften über den Datenschutz. Zuständig dafür ist das Innenministerium.
Die EU-DSGVO ist am 24.05.2016 in Kraft getreten und gilt ab dem 25. Mai 2018 und fällt somit in die Projektlaufzeit von enera. Daher muss die die EU-DSGVO in enera berücksichtigt werden. Diese Verordnung wird über das DSAnpUG-EU ins deutsche Recht übernommen, so dass die Verabschiedung dieses Gesetzes abgewartet werden muss. Der Zeitplan[15] sieht einen Abschluss des Prozesses im Mai 2017 vor.

2.1.8 EEG

Das EEG ist das Erneuerbare-Energien-Gesetz für den Ausbau der Erneuerbaren Energien. Dieser Ausbau soll laut § 1 „stetig, kosteneffizient und netzverträglich erfolgen“ und damit die Ziele der EU bzgl. des Anteils an erzeugtem Strom aus erneuerbaren Energien erfüllen. Auf Informationssicherheitsaspekte wird in diesem Gesetz nicht explizit eingegangen. In verschiedene Paragraphen wird auf das MsbG und somit den Stand der Technik und das BSI verwiesen.

2.1.9 KWKG

Das KWKG ist das Kraft-Wärme-Kopplungsgesetz und dient der Erhaltung, der Modernisierung und dem Ausbau der Kraft-Wärme-Kopplung. Auch das KWKG verweist nicht explizit auf Informationssicherheitsmaßnahmen und bezieht sich an verschiedenen Stellen auf das MsbG, so dass auch hier der Stand der Technik umgesetzt werden muss, der teilweise durch das BSI vorgegeben wird.

2.1.10 Zusammenfassung „Gesetze und Verordnungen“

In der folgenden Tabelle 1 sind die in diesem Abschnitt 2.1 beschriebenen Gesetze und Verordnungen überblicksartig dargestellt, wobei ihre geografische Gültigkeit eingeordnet und der entsprechende Inhalt in Bezug auf Informationssicherheit kurz erläutert wird.

[15] Siehe z.B. hier: https://dsgvo.expert/aktueller-fahrplan-fuer-dsanpug-eu-inkl-bdsg-neu/.

Name Gesetz	Gültigkeit			Inhalt – kurz
	regional	national	international	
IT-Sicherheitsgesetz		x		Vorgaben für den Schutz von kritischen Infrastrukturen; Meldepflichten etc.
BSI-Gesetz		x		Vorgaben für Aufgaben und Befugnisse des BSI; Nachweis Stand der Technik, BSI als zentrale Meldestelle etc.
EU-NIS-Richtlinie			x	Vorgaben für Netz- und Informationssicherheit in Europa; Umsetzung und Gewährleistung von Mindestanforderungen etc.
EnWG		x		Vorgaben zu IT-Sicherheit an Netz- und Anlagenbetreiber; Anwendung des IT-Sicherheitskatalogs und MsbG etc.
IT-Sicherheitskatalog		x		Vorgaben zu Informationssicherheit für Strom- und Gasnetzbetreiber; Betrieb eines ISMS nach DIN ISO/IEC 27001/27002/27019 etc.
MsbG		x		Vorgaben zu Sicherheitsanforderungen für Messeinrichtungen der Energieversorgung; Umsetzung durch Schutzprofile und TRs des BSI etc.
NDSG	x			Datenschutzvorgaben in Niedersachsen
BDSG		x		Datenschutzvorgaben in Deutschland
EU-DSGVO			x	Datenschutzvorgaben in der Europäischen Union
EEG		x		Indirekte Vorgaben zu Informationssicherheit
KWKG		x		Indirekte Vorgaben zu Informationssicherheit

Tabelle 1: Übersicht „Gesetze und Verordnungen“

In der folgenden Tabelle 2 werden die Gesetze, die Informationssicherheitsaspekte behandeln, den einzelnen Arbeitspaketen (AP) innerhalb des enera-Projekts zugeordnet und somit deren Relevanz für die einzelnen APs aufgezeigt. Dabei ist jeder AP-Nummer ein Kurztitel zur besseren Verständlichkeit angehängt. Diese Zuordnung zu den APs erfolgte im Rahmen von AS 12.2.1 und soll durch die Schnittstellenverantwortlichen für Informationssicherheit in den APs überprüft werden. Ein „x“ pro Zelle bedeutet dabei, dass das entsprechende Gesetz eine Relevanz für das AP aufweist. Ein „(x)“ pro Zelle heißt, dass das entsprechende Gesetz eine Relevanz für das AP ausweisen kann bzw. es gibt eine indirekte Relevanz des Gesetzes für das AP.

AP-Nummer – Kurztitel	IT-Sicherheitsgesetz	EU-NIS-Richtlinie	BSI-Gesetz	EnWG	IT-Sicherheitskatalog	MsbG	Datenschutz-gesetze			EEG	KWKG
							NDSG	BDSG	EU-DSGVO		
AP1 – Digitale Konnektivität	x	x	x	x	x	x	x	x	x		
AP2 – SDSP	(x)	(x)	(x)		(x)	(x)	x	x	x		
AP3 – SG-Operator	x	x	x	x	x		x	x	x		
AP4 – Rollout Netzbetriebsmittel	x	x	x	x	x	(x)					
AP5 – Flexibilisierung	x	x	x	x	x	(x)	(x)	(x)	(x)		
AP6 – Technische Entwicklung regionaler Produkte	x	x	x	x	x	x	x	x	x		
AP7 – Marktintegration regionaler Produkte							x	x	x		
AP8 – Energierecht											
AP9 – Neue Geschäftsmodelle							x	x	x		
AP10 – enera Qualifizierungscenter							x	x	x		
AP11 – Bürgerbeteiligung						(x)	x	x	x		
AP12 – Architektur und Security	x	x	x	x	x	x	x	x	x		
AP13 – Nationaler/Internat. Transfer									x		
AP14 – Projektmanagement											

Tabelle 2: Relevanz der Gesetze für die einzelnen APs in enera

2.2 Normen, Standards und Richtlinien

Dieser Abschnitt 2.2 beschreibt verschiedene Normen, Standards und Richtlinien für Informationssicherheit, die für das Projekt enera relevant sind. In den Abschnitten 2.2.1 bis 2.2.12 werden die identifizierten Normen, Standards und Richtlinien kurz beschrieben. Abschnitt 2.2.13 gibt abschließend eine Übersicht und Zusammenfassung zu den Standards, um die Relevanz für das Projekt zu erläutern.

2.2.1 ISO/IEC 27000-Reihe

ISO steht für „International Organization for Standardization“ (deutsch: Internationale Organisation für Normung) und ist eine internationale Vereinigung von Normungsorganisationen, die internationale Normen erarbeitet. Die IEC, auf Deutsch „Internationale Elektrotechnische Kommission“ ist ein internationales Normungsgremium, das Standards und Normen für den Bereich der Elektrotechnik und der Elektronik entwickelt. Sowohl die ISO als auch die IEC haben ihren Sitz in Genf in der Schweiz.

Die ISO/IEC 27000-Reihe (auch mit ISO/IEC 27000-Familie bezeichnet) ist eine Reihe von Standards zur Informationssicherheit, welche von der International Organization for Standar-

dization (ISO[16]) und der International Electrotechnical Commission (IEC[17]) herausgegeben wird.

2.2.1.1 ISO 27000

Die internationale Norm ISO/IEC 27000 bildet den Rahmen für die ISO/IEC 27000-Familie. Sie definiert häufig verwendete Fachbegriffe und gibt einen Kurzüberblick über die einzelnen Standards.

2.2.1.2 ISO 27001

Die internationale Norm ISO/IEC 27001 (deutsche Fassung DIN ISO/IEC 27001) wurde erarbeitet, um Anforderung für die Einrichtung, Implementierung, Wartung und laufende Verbesserung eines **Informationssicherheitsmanagementsystems (ISMS)** festzulegen.
Mit diesem sollen Vertraulichkeit, Integrität und Verfügbarkeit von Informationen durch Anwendung eines Risikomanagement-Prozesses geschützt werden und interessierte Parteien sollen darauf vertrauen können, dass mit Risiken angemessen umgegangen wird.
Die Norm kann von internen und externen Parteien – darunter Zertifizierungsstellen – dazu eingesetzt werden, die Fähigkeit einer Organisation zur Einhaltung ihrer eigenen Informationssicherheitsanforderungen zu bewerten.
DIN ISO/IEC 27001 beinhaltet Anforderungen an ein ISMS, das mittelbar zur Informationssicherheit beiträgt. Da das Dokument sehr generisch gehalten ist, um auf alle Organisationen unabhängig von Typ, Größe und Geschäftsfeld anwendbar zu sein, haben diese Anforderungen einen niedrigen technischen Detaillierungsgrad, wobei die Anforderungen an die Prozesse wohl definiert sind.
Folgende, in den Abschnitten 4 bis 10 der Norm genannten Anforderungen spiegeln zusammengenommen den **Plan-Do-Check-Act Zyklus** (vgl. Abbildung 1 in Abschnitt 2.2.2.1) wieder und müssen von einer Organisation erfüllt werden um Konformität zur Norm zu erlangen, siehe Tabelle 3:

Thema	Subthemen	Erläuterung
4 Kontext der Organisation	4.1 Verständnis der Organisation und ihres Kontextes 4.2 Verständnis der Bedürfnisse und Erwartungen interessierter Parteien 4.3 Festlegung des Geltungsbereichs des ISMS 4.4 ISMS	Definition der Anforderungen, um externe und interne Belange und Wünsche der Beteiligten zu verstehen und den Umfang des ISMS zu definieren
5 Führung	5.1 Führung und Engagement 5.2 Leitlinie 5.3 Organisatorische Aufgaben, Zuständigkeiten und Befugnisse	Festlegung von Rollen und Verantwortlichkeiten, und der Inhalte der obersten IT-Sicherheitsrichtlinien

[16] Siehe https://www.iso.org.
[17] Siehe http://www.iec.ch/.

Thema	Subthemen	Erläuterung
6 Planung	6.1 Maßnahmen zum Umgang mit Risiken und Chancen 6.2 Informationssicherheitsziele und Pläne für deren Erreichung	Definition der Anforderungen für Risikomanagement, Erklärung zur Anwendbarkeit, und Bestimmung der Ziele der Informationssicherheit
7 Unterstützung	7.1 Ressourcen 7.2 Kompetenz 7.3 Bewusstsein 7.4 Kommunikation 7.5 Dokumentierte Informationen	Anforderungen für das Schutzziel Verfügbarkeit von Ressourcen, Kompetenzen, Bewusstsein, Kommunikation und Kontrolle von Dokumenten und Einträgen
8 Einsatz/ Betrieb	8.1 Einsatzplanung und -kontrolle 8.2 Informationssicherheitsrisikoeinschätzung 8.3 Informationssicherheitsrisikobehandlung	Anforderungen an Risikobehandlung und Sicherheitsmaßnahmen
9 Leistungsauswertung	9.1 Überwachung, Messung, Analyse und Auswertung 9.2 Internes Audit 9.3 Prüfung durch die Leitung	Anforderungen für Überwachung, Messung, Analyse und Bewertung, interne Audits und Managementprüfung
10 Verbesserung	10.1 Fehler und Korrekturmaßnahmen 10.2 Laufende Verbesserung	Anforderungen für Abweichungen, Korrekturen, und kontinuierliche Verbesserung

Tabelle 3: Anforderungen des Plan-Do-Check-Act Zyklus

2.2.1.3 ISO 27002

Diese Internationale Norm wurde erarbeitet, um Organisationen als Referenz zur Auswahl von Maßnahmen bei der Einführung eines **Informationssicherheitsmanagementsystems (ISMS)** nach ISO/IEC 27001 zu dienen oder als Leitfaden für Organisationen, die gemeinhin akzeptierte Maßnahmen für die Informationssicherheit einführen möchten. Sie enthält Richtlinien für organisatorische Normen und Managementpraktiken bezüglich Informationssicherheit, einschließlich Auswahl, Implementierung und Management von Sicherheitsmaßnahmen unter Berücksichtigung des Umfelds der Informationssicherheitsrisiken in einer Organisation.
Das Dokument ist gut strukturiert und gliedert sich in 14 Abschnitte („clauses“) über Sicherheitsmaßnahmen („controls“) mit 35 Hauptkategorien („main security categories“) der Sicherheit und 113 Sicherheitsmaßnahmen.
Jede Hauptkategorie von Sicherheitsmaßnahmen enthält:

- Zielsetzung einer Sicherheitsmaßnahme und was erreicht werden soll („control objective“)
- Eine oder mehrere Sicherheitsmaßnahme(n), die zur Erreichung der Zielsetzung angewendet werden können.

Die Beschreibungen der Sicherheitsmaßnahmen sind wie folgt strukturiert:

- Maßnahme („control“)
  Definition der spezifischen Sicherheitsmaßnahme und Erklärung, wie das Ziel der Maßnahme erreicht wird.
- Umsetzungshinweise („implementation guidance“)

Detaillierte (aber weniger detailliert als Grundschutzmaßnahmen des BSI) Information zur Umsetzung von Sicherheitsmaßnahmen und um ihre Ziele zu erreichen. Es wird ausdrücklich darauf aufmerksam gemacht, dass die Umsetzungshinweise vielleicht nicht in allen Situationen ausreichend sind, möglicherweise nicht die spezifische Sicherheitsanforderungen einer Organisation erfüllen oder nur eingeschränkt anwendbar sein könnten.

- Weitere zu berücksichtigende Informationen, wie rechtliche Aspekte und Verweise auf andere Normen

Folgende Abschnitte und Hauptkategorien von Sicherheitsmaßnahmen werden behandelt, siehe Tabelle 4:

Nr.	Abschnitt	Hauptkategorie(n)
5	Sicherheitsleitlinien	• Managementausrichtung zur Informationssicherheit
6	Organisation der Informationssicherheit	• Interne Organisation • Mobilgeräte und Telearbeit
7	Personalsicherheit	• Vor der Anstellung • Während der Anstellung • Beendigung und Wechsel der Anstellung
8	Management von organisationseigenen Werten (assets)	• Verantwortung für organisationseigene Werte • Klassifizierung von Informationen • Handhabung von Speicher- und Aufzeichnungsmedien
9	Zugriffskontrolle	• Geschäftliche Anforderungen in Bezug auf die Zugriffskontrolle • Benutzerverwaltung • Benutzerverantwortung • Kontrolle des Zugangs zu Systemen und Anwendungen
10	Kryptographie	• Kryptographische Maßnahmen
11	Schutz vor physischem Zugang und Umwelteinflüssen	• Sicherheitsbereiche • Sicherheit von Betriebsmitteln
12	Betriebssicherheit	• Betriebsverfahren und Zuständigkeiten • Schutz vor Malware • Backup • Protokollierung und Überwachung • Kontrolle von Betriebssoftware • Technisches Schwachstellenmanagement • Auswirkungen von Audits auf Informationssysteme
13	Sicherheit in der Kommunikation	• Netzwerksicherheitsmanagement • Informationsübertragung
14	Anschaffung, Entwicklung und Instandhaltung von Systemen	• Sicherheitsanforderungen für Informationssysteme • Sicherheit in Entwicklungs- und Unterstützungsprozessen • Prüfdaten
15	Lieferantenbeziehungen	• Informationssicherheit bei Lieferantenbeziehungen • Management der Dienstleistungserbringung durch Lieferanten

Nr.	Abschnitt	Hauptkategorie(n)
16	Management von Informationssicherheitsvorfällen	• Management von Informationssicherheitsvorfällen und Verbesserungen
17	Informationssicherheitsaspekte des Betriebskontinuitätsmanagements	• Aufrechterhaltung der Informationssicherheit • Redundanzen
18	Richtlinienkonformität	• Einhaltung gesetzlicher und vertraglicher Anforderungen • Informationssicherheitsprüfungen

Tabelle 4: Abschnitte und Hauptkategorien des ISO/IEC 27002

2.2.1.4 ISO/IEC 27019

Die ISO/IEC TR 27019:2015-03 (DIN SPEC 27019:2015-03) ist eine Erweiterung der Norm ISO/IEC 27002 auf den Bereich der Prozessleit- und Automatisierungstechnik in der Energieversorgung. Sie ergänzt und vertieft dies in Bezug auf Prozesssteuerungssysteme und Netzwerke zur Steuerung und Überwachung von Erzeugung, Übertragung und Verteilung von Strom, Gas und Wärme in Kombination mit der Steuerung von unterstützenden Prozessen. Die Norm ist anwendbar auf Leit- und Automatisierungssysteme, Schutz- und Safetysysteme sowie Messtechnik inklusive der zugehörigen Kommunikations- und Fernwirktechnik.

Folgende Maßnahmen ergänzen die ISO/IEC 27002 hinsichtlich der Erfordernisse im Bereich Energieversorgung (die Nummerierung bezieht sich dabei auf die ISO/IEC 27002:2005), siehe Tabelle 5:

Nr.	Titel	Beschreibung
9.1.7	Sichern von Leitstellen	Maßnahmen zur physischen Sicherheit von Leitstellen mit zentralen Prozesssteuerungssystemen wie Steuerungsservern, MMI-Systemen und unterstützenden Systemen, sollten konzipiert, entwickelt und umgesetzt werden.
9.1.8	Sicherung von Technikräumen	Maßnahmen zur physischen Sicherheit von Technikräumen für Prozesssteuerungssysteme der Energieversorgung sollten konzipiert, entwickelt und umgesetzt werden.
9.1.9	Sicherung von Außenstandorten	Maßnahmen zur physischen Sicherheit von Außenstandorten, an denen Prozesssteuerungssysteme der Energieversorgung betrieben werden, sollten konzipiert, entwickelt und umgesetzt werden.
9.3.1	Betriebseinrichtung in Bereichen anderer Energieversorger	Wenn Energieversorger Betriebseinrichtungen außerhalb der eigenen Gelände oder Räumlichkeiten in den Verantwortungsbereichen anderer Versorger betreiben, wie beispielsweise in Übergabestationen, sollte die Betriebseinrichtung in einem gesicherten Bereich positioniert werden, so dass die Risiken von umgebungsbezogenen Bedrohungen oder Gefahren und eines nicht autorisierten Zugriffs reduziert werden.
9.3.2	Betriebseinrichtung beim Kunden vor Ort	Wenn Energieversorger Betriebseinrichtungen beim Kunden vor Ort betreiben, z. B. um die Energielieferung zu steuern, zu messen und/oder um zusätzliche Dienste bereitzustellen, sollte die Betriebseinrichtung geschützt werden, so dass die Risiken von umgebungsbezogenen Bedrohungen oder Gefahren und eines nicht autorisierten Zugriffs reduziert werden.

Nr.	Titel	Beschreibung
9.3.3	Gekoppelte Steuerungs- und Kommunikationssysteme	Wenn Prozesssteuerungssysteme und zugehörige Kommunikationsverbindungen mit denen von externen Dritten gekoppelt werden, sollten die Verantwortungsgrenzen und Schnittstellen zu allen externen Beteiligten von den Kunden klar definiert und spezifiziert werden, so dass jedes Unternehmen in einem angemessenen Zeitraum abgetrennt und isoliert werden kann, um identifizierte bekannte Risiken abzuwenden.
10.6.3	Sicherung der Prozessdatenkommunikation	Maßnahmen zur Sicherstellung der Vertraulichkeit, Integrität und Verfügbarkeit der internen und externen Prozessdatenkommunikation sollten in Abhängigkeit der Sensibilität der übertragenen Daten konzipiert, entwickelt und umgesetzt werden.
10.11.1	Behandlung von Altsystemen	Alle herkömmlichen Prozesssteuerungssystemtechnologien, Systeme und Komponenten (Legacy-Systeme) sollten mit ihren potentiellen Informationssicherheitsschwachstellen identifiziert werden. Zur Minderung der identifizierten Risiken von alten Prozesssteuerungssystemtechnologien und Prozesssteuerungssystemen sollten entsprechende Maßnahmen umgesetzt werden.
10.12.1	Integrität und Verfügbarkeit von Funktionen der Betriebssicherheit	Die Integrität und Verfügbarkeit von Informationswerten (Information Assets), Systemen, Komponenten und Funktionen, die zur Sicherstellung der Betriebssicherheit (Safety) benötigt werden, sollte im Einklang mit den branchenspezifischen Normen und Gesetzen sichergestellt werden.
11.4.8	Logische Anbindung von externen Prozesssteuerungssystemen	Vor der logischen Kopplung von Prozesssteuerungssystemen und den zugehörigen Kommunikationsverbindungen mit externen Dritten, sollte vom Energieversorger sichergestellt werden, dass ausschließlich erlaubte Kommunikation und Informationsflüsse sowie berechtigte Steuerbefehle und Meldungen über die Kommunikationsverbindung ausgetauscht werden können. Das durch die Kopplung resultierende Risiko sollte entsprechend bewertet werden.
14.2.1	Notfall-Kommunikation	Im Falle von Großstörungen, Naturkatastrophen, Unfällen oder anderen möglichen Notfallsituationen oder wenn das Risiko eines Eintretens eben dieser besteht, sollten Energieversorger sicherstellen, dass wichtige Kommunikationsverbindungen mit dem eigenen Notfallpersonal oder dem Notfallpersonal anderer Versorger, wichtigen Prozesssteuerungssystemen und externen Notfall-Organisationen, die zum Schutz, zur Behandlung oder zur Wiederherstellung nach solchen Vorfällen notwendig sind, zur Verfügung stehen.

Tabelle 5: Ergänzende Maßnahmen der ISO/IEC 27019 in Bezug auf die ISO/IEC 27002

2.2.2 BSI Grundschutz

Im Bearbeitungszeitraum des AS12.2.1 besteht der BSI IT-Grundschutz aus den BSI-Standards

- 100-1: Managementsysteme für Informationssicherheit

- 100-2: IT-Grundschutz-Vorgehensweise
- 100-3: Risikoanalyse auf der Basis von IT-Grundschutz
- 100-4: Notfallmanagement

und den IT-Grundschutzkatalogen, Stand 15. Ergänzungslieferung.
Diese Dokumente enthalten Empfehlungen des BSI zu Methoden, Prozessen und Verfahren sowie Vorgehensweisen und Maßnahmen mit Bezug zur Informationssicherheit.
Der Kerngedanke des IT-Grundschutzes ist die Vorgabe von Standardsicherheitsmaßnahmen für einen **Informationsverbund** mit normalem Schutzbedarf, ohne dass dafür zunächst eine dedizierte Risikoanalyse durchgeführt werden muss. Es wird angenommen, dass – für bestimmte weit verbreitete Technologien und übliche Einsatzszenarien – den relevanten Gefährdungen durch die Grundschutzmaßnahmen ausreichend begegnet werden kann. Dieses pauschalierte Vorgehen erlaubt zum einen die schnelle Bestimmung der notwendigen Maßnahmen und zum anderen steht ein sehr umfangreicher Fundus an detailliert ausformulierten Standardmaßnahmen aus den Bereichen Infrastruktur, Organisation, Personal, Hardware, Software, Netze und Notfallvorsorge zur Verfügung.
Im Jahr 2017 wird der IT-Grundschutz modernisiert. Stand April 2017 liegen „BSI-Standard 200-2 IT-Grundschutzmethodik“ und „BSI-Standard 200-3 Risikoanalyse auf der Basis von IT-Grundschutz“ als Community Draft vor. Zu den Grundschutzkatalogen liegen ca. 30 Entwürfe und Community Drafts vor.
Bei der Beschreibung der einzelnen Standards und Bausteine wird im Folgenden auch auf die zukünftige (geplante) Version eingegangen.

2.2.2.1 BSI-Standard 100-1: Managementsysteme für Informationssicherheit

Der Standard beschreibt, wie ein Informationssicherheitsmanagementsystem (ISMS) grundsätzlich in einer Organisation aufgebaut werden kann. Der PDCA-Zyklus (Plan, Do, Check Act) wird erläutert (siehe Abbildung 1).

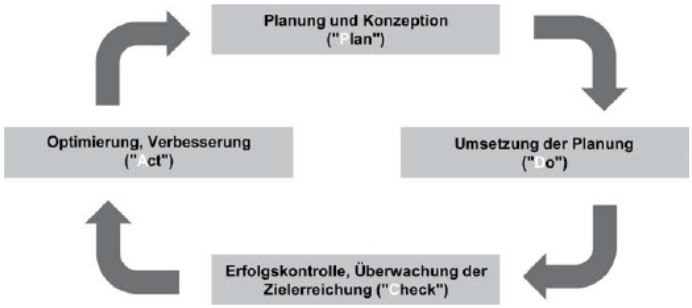


Abbildung 1: PDCA-Zyklus (Quelle: BSI-Standard 100-1)

Weitere wichtigste Elemente und Grundbegriffe eines ISMS werden erläutert und in Zusammenhang gebracht. Darunter fallen die Themen:

- Standards zur Informationssicherheit
- Informationssicherheitsprozess
- Informationssicherheitsorganisation
- Sicherheitskonzept
- Managementprinzipien

- Ressourcen für Informationssicherheit
- Leitlinie zur Informationssicherheit

2.2.2.2 BSI-Standard 100-2 / 200-2: IT-Grundschutzmethodik

Die IT-Grundschutz-Vorgehensweise beschreibt Schritt für Schritt, wie ein Managementsystem für Informationssicherheit in der Praxis aufgebaut und betrieben werden kann. Die Aufgaben des Informationssicherheitsmanagements und der Aufbau einer Organisationsstruktur für Informationssicherheit sind dabei wichtige Themen. Die IT-Grundschutz-Vorgehensweise geht sehr ausführlich darauf ein, wie ein Sicherheitskonzept in der Praxis erstellt werden kann, wie angemessene Sicherheitsmaßnahmen ausgewählt werden können und was bei der Umsetzung des Sicherheitskonzeptes zu beachten ist. Die einzelnen Schritte sind:

1. **Festlegen des Informationsverbundes**

Ein Informationsverbund soll alle organisatorischen Maßnahmen, personellen Ressourcen sowie technischen und infrastrukturellen Komponenten umfassen, die zur Unterstützung einer oder mehrerer Fachaufgaben, Geschäftsprozesse oder Organisationseinheiten dienen.

2. **IT-Strukturanalyse**

Die im festgelegten Informationsverbund genutzten Anwendungen, die vorhandene Infrastruktur und Informations- und Kommunikationstechnik sowie die organisatorischen und personellen Rahmenbedingungen werden strukturiert erfasst. Dazu gehören auch eine Netzplanerhebung und die Komplexitätsreduktion durch Gruppenbildung. Die IT-Strukturanalyse dient der Erhebung von Informationen, die für die weitere Vorgehensweise in der Erstellung eines IT-Sicherheitskonzepts nach ISO 27001 / IT-Grundschutz benötigt werden.

3. **Feststellung des Schutzbedarfs**

In der Schutzbedarfsfeststellung wird nach der Definition der Schutzbedarfskategorien für die bei der IT-Strukturanalyse erfassten Objekte im Informationsverbund entschieden, welchen Schutzbedarf sie bezüglich der Vertraulichkeit, Integrität und Verfügbarkeit besitzen. Dieser Schutzbedarf orientiert sich an den möglichen Schäden, die mit einer Beeinträchtigung der betroffenen Anwendungen und damit der jeweiligen Geschäftsprozesse verbunden sind.
Aus den Ergebnissen der Schutzbedarfsfeststellung werden Schlussfolgerungen hinsichtlich der Notwendigkeit und dem Umfang einer ergänzenden Sicherheitsanalyse gezogen und ggf. werden zusätzliche Empfehlungen ausgesprochen, z.B. zur Aufteilung in Sicherheitszonen.

4. **Modellierung nach IT-Grundschutz**

Die Modellierung besteht darin, Zielobjekten bzw. Gruppen von Zielobjekten Bausteine des IT-Grundschutzes zuzuordnen. Sollten Zielobjekte existieren, die nicht mit den Original-Grundschutzbausteinen modelliert werden können, können soweit möglich, ähnliche Bausteine herangezogen werden.

5. **Basis-Sicherheitscheck I**

Der Basissicherheitscheck (Soll-Ist-Vergleich) ist die zentrale Aufgabe des IT-Sicherheitskonzepts nach BSI IT-Grundschutz. Er dient zur Feststellung des Umsetzungsgrades der zutreffenden Standard-Sicherheitsmaßnahmen.

Nach organisatorischen Vorarbeiten (Sichtung relevanter hausinterner Papiere, z. B. Organisationsverfügungen, Arbeitshinweise, Sicherheitsanweisungen, Handbücher; Ermittlung geeigneter Interviewpartner, Entscheidung über die Beteiligung externer) wird, unter Verwendung des Grundschutzmodells als Prüfplan, ein Soll-Ist-Vergleich durchgeführt, in welchem der Umsetzungsgrad der Standardsicherheitsmaßnahmen festgestellt wird.

6. Ergänzende Sicherheitsanalyse

Ziel des IT-Grundschutzes ist es, durch infrastrukturelle, organisatorische, personelle und technische Standard-Sicherheitsmaßnahmen ein Standard-Sicherheitsniveau für IT-Systeme aufzubauen, das auch für Bereiche mit erhöhtem Schutzbedarf ausbaufähig ist.
Ergänzende Sicherheitsanalysen sind durchzuführen, wenn

- die Schutzbedarfskategorie "hoch" oder "sehr hoch" in mindestens einem der Grundwerte vorliegt,
- zusätzlicher Analysebedarf besteht (z. B. bei besonderem Einsatzumfeld) oder
- für bestimmte Komponenten oder Aspekte kein geeigneter Baustein in den IT-Grundschutzkatalogen existiert.

Das Ziel ist dabei, für die einzelnen Zielobjekte jeweils zu entscheiden, ob weitere Risikobetrachtungen erforderlich sind.

7. Basis-Sicherheitscheck II

Als Ergebnis der durchgeführten Risikoanalyse wurden (möglicherweise) zusätzlich zu den Standardsicherheitsmaßnahmen weitergehende, ergänzende Sicherheitsmaßnahmen identifiziert. Diese werden einem zweiten Basis-Sicherheitscheck unterzogen.

8. Konsolidierung und Umsetzungsplanung

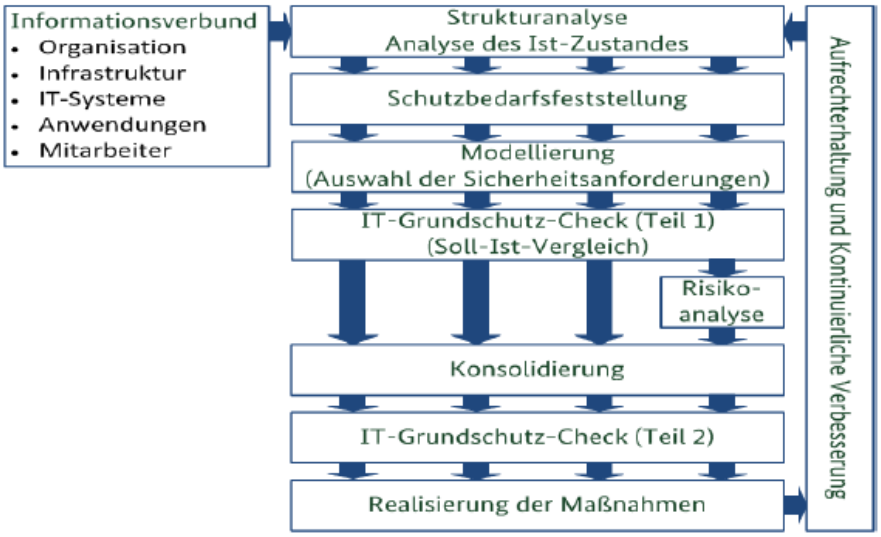
In diesem Schritt werden die noch umzusetzenden Sicherheitsmaßnahmen konsolidiert. Da im IT-Grundschutz für eine Vielzahl von verschiedenen Organisationsformen und technischen Ausgestaltungen Empfehlungen gegeben werden, müssen die ausgewählten Maßnahmen eventuell noch konkretisiert bzw. an die organisatorischen und technischen Gegebenheiten des Kunden angepasst werden. Für nicht vollständig umgesetzte Maßnahmen wird eine Priorisierung vorgenommen und ein Zeitplan für ihre Realisierung erstellt. Verantwortliche für die Initiierung und die Umsetzung werden festgelegt.

BSI-Standard 200-2

Der BSI-Standard 200-2 löst voraussichtlich im Oktober 2017 den BSI-Standard 100-2 ab. Ein Community Draft liegt bereits vor.
Im Rahmen der Modernisierung des IT-Grundschutzes wurden neben der Standard-Absicherung (welche im Wesentlichen der IT-Grundschutzvorgehensweise des BSI-Standard 100-2 entspricht, siehe Abbildung 2) die Vorgehensweisen zur Basis-Absicherung und Kern-Absicherung hinzugefügt. Weitere Neuerungen sind:

- Wegfall der ergänzenden Sicherheitsanalyse als eigener Schritt der Grundschutzmethodik
- Erweiterung um Virtualisierung, Cloud-, Industrial-Control-Systems- (ICS) und Internet-of-Things- (IoT) -Absicherung
- Klarstellung der Rollen und Aufgaben von IT-Sicherheitsbeauftragten (IT-SiBe) und Informationssicherheitsbeauftragten (ISB)

- Anpassungen an Fortschreibung der ISO-Standards
- Betonung der Informationsklassifizierung
- Überarbeitung des Informationsflusses im Informationssicherheitsprozess, Angleichung mit BSI-Standard 100-4



Quelle: BSI 200-2

Abbildung 2: Erstellung eines IT-Sicherheitskonzepts mit der Standard-Absicherung (BSI-Standard 100-2)

2.2.2.3 BSI-Standard 100-3 / 200-3: Risikoanalyse auf der Basis von IT-Grundschutz

Gemäß BSI-Standard 100-3 wird aufbauend auf der durchgeführten ergänzenden Sicherheitsanalyse und der damit einhergehenden Managemententscheidung für die in Frage kommenden Zielobjekte eine Risikoanalyse durchgeführt, mit den Schritten:

- Gefährdungsübersicht
- Zusätzliche Gefährdungen
- Gefährdungsbewertung
- Risikobehandlung
- Konsolidierung

Seit Oktober 2016 liegt BSI-Standard 200-3 als Nachfolgestandard zu BSI-Standard 100-3 als Community Draft vor. Die wesentlichen Neuerungen betreffen:

- Risikoanalyse auf Basis der elementaren Gefährdungen umgestellt
- Einführung Risikomanagementsystem
- Einführung Matrix-Ansatz zur Bewertung von Risiken
- Einführung Risikoappetit und Chancenmanagement

Die Einordnung der Risikoanalyse in den Sicherheitsprozess ist Abbildung 3 zu entnehmen.

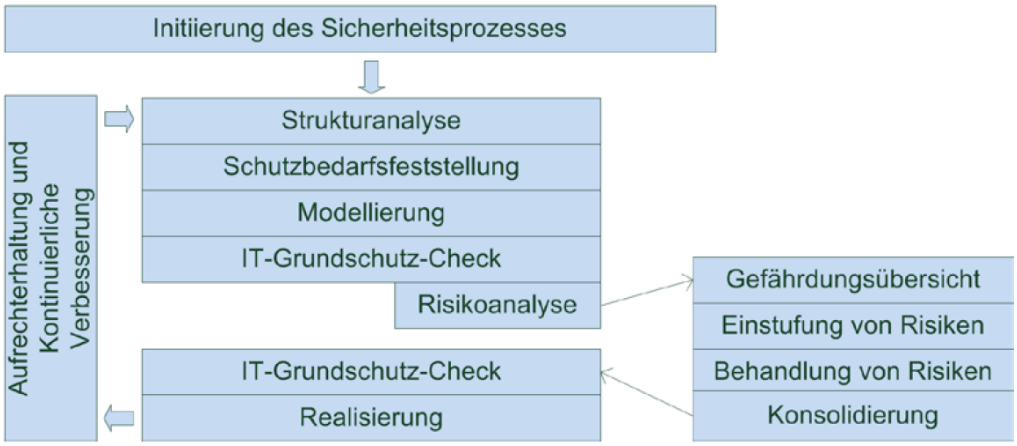


Abbildung 3: Einordnung der Risikoanalyse in den Sicherheitsprozess (Quelle: BSI-Standard 200-3)

2.2.2.4 BSI-Standard 100-4 Notfallmanagement

Mit dem BSI-Standard 100-4 wird ein systematischer Weg aufgezeigt, ein Notfallmanagement in einer Behörde oder einem Unternehmen aufzubauen, um die Kontinuität des Geschäftsbetriebs sicherzustellen. Aufgaben eines Notfallmanagements sind daher, die Ausfallsicherheit zu erhöhen und die Institution auf Notfälle und Krisen adäquat vorzubereiten, damit die wichtigsten Geschäftsprozesse bei Ausfall schnell wieder aufgenommen werden können. Es gilt, Schäden durch Notfälle oder Krisen zu minimieren und die Existenz der Behörde oder des Unternehmens auch bei einem größeren Schadensereignis zu sichern.
Der Standard BSI-Standard 100-4 ist relativ komplex und seine Umsetzung mit recht hohem Aufwand verbunden. Deshalb hat das BSI im Nachgang ein „Umsetzungsrahmenwerk zum Notfallmanagement nach BSI-Standard 100-4“ herausgegeben.

2.2.2.5 IT-Grundschutzkataloge / IT-Grundschutzkompendium

In den IT-Grundschutz-Katalogen werden Standard-Sicherheitsmaßnahmen für typische Infrastrukturobjekte, Geschäftsprozesse, Anwendungen, IT-Systeme und Netze empfohlen. Ziel ist es, einen angemessenen Schutz für alle Informationen einer Institution zu erreichen, indem infrastrukturbezogene, organisatorische, personelle und technischen Standard-Sicherheitsmaßnahmen als Gesamtes angewendet werden.
Die Standardsicherheitsmaßnahmen sind in den Katalogen als Bausteine strukturiert. Jeder Baustein deckt ein bestimmtes Themengebiet ab und enthält die darauf wirkenden Gefährdungen und die umzusetzenden Sicherheitsmaßnahmen. Dabei sind die Gefährdungen in die Kategorien

- Höhere Gewalt
- Organisatorische Mängel
- Menschliches Versagen
- Technisches Versagen
- Vorsätzliche Handlungen

strukturiert. Sicherheitsmaßnahmen sind hinsichtlich ihrer Bedeutung/Dringlichkeit mit (A), (B), (C), (Z) oder (W) gekennzeichnet. (A)-Maßnahmen sind am wichtigsten, (Z)-Maßnahmen gehen über den reinen Grundschutz hinaus.

Die Grundschutzkataloge der 15. Ergänzungslieferung enthalten 88 Bausteine in den 5 Schichten

- Übergreifende Aspekte
- Infrastruktur
- IT-Systeme
- Netze
- Anwendungen

Ein Baustein enthält ca. 5 – 20 Gefährdungen und ca. 5 bis 50 Maßnahmen, wobei Maßnahmen zum Teil sehr ausführlich formuliert sind und auch technisch ins Detail gehen können. Diese genauen Vorgaben haben den Vorteil, dass sie einem Verantwortlichen eine starke Unterstützung bei der Implementierung der richtigen Mechanismen bieten können, was auch daran zu erkennen ist, dass die Grundschutzkataloge auch außerhalb der IT-Grundschutzmethodik Verwendung finden, z.B. greifen auch einige Security Manager beim Aufbau eines ISMS nach der internationalen Norm ISO 27001 darauf zurück.

Die Nachteile der detaillierten Maßnahmenkataloge liegen in dem für das BSI kaum zu leistenden Pflegeaufwand und der in einigen Anwendungsfeldern zu geringen Flexibilität. Daher werden im Zuge der Modernisierung des IT-Grundschutzes die IT-Grundschutzkataloge durch das IT-Grundschutz-Kompendium ersetzt.

IT-Grundschutz-Kompendium

Im IT-Grundschutz-Kompendium werden die neuen Bausteine nach zehn Schichten, die wiederum in die folgenden Prozess- und Systembausteine unterteilt sind, strukturiert.

Prozessbausteine

- CON - Konzepte & Vorgehensweisen
- DER - Detektion & Reaktion
- ISMS - Sicherheitsmanagement
- OPS - Betrieb
- ORP - Organisation & Personal

Systembausteine

- APP – Anwendungen
- IND - Industrielle IT
- INF - Infrastruktur
- NET - Netze
- SYS - IT-Systeme

Ein Baustein ist nun kompakt und ohne Verweise in weitere Bereiche der IT-Grundschutz-Kataloge. Er enthält spezifische Gefährdungen und Sicherheitsanforderungen (keine Maßnahmen mehr) für den jeweiligen Bereich. Die Sicherheitsanforderungen sind deutlich kürzer formuliert als die bisherigen Sicherheitsmaßnahmen und sie schreiben auch nicht mehr explizit vor, wie ein bestimmtes Sicherheitsziel erreicht werden muss.

Um dennoch auf die gewaltige Wissensbasis, welche die bisherigen Maßnahmen darstellen nicht verzichten zu müssen, wird es zukünftig neben den Bausteinen Umsetzungshinweise geben, in denen zu den Anforderungen die passenden Sicherheitsmaßnahmen aufgezeigt werden, also wie etwas getan werden kann.

Die Anforderungen der Bausteine werden zukünftig in drei Kategorien gegliedert: Basis-, Standard- und Anforderungen für einen höheren Schutzbedarf. Vorrangig sollten die Basis-Anforderungen umgesetzt werden, da sie mit geringem Aufwand den größtmöglichen Nutzen erzielen. Darauf aufbauend vervollständigen die Standard-Anforderungen den **Stand der Technik** und adressieren den normalen Schutzbedarf. Ergänzend dazu enthalten die modernisierten Bausteine Beispiele für Sicherheitsanforderungen bei hohem Schutzbedarf.

2.2.2.6 IT-Grundschutz-Profile im modernisierten IT-Grundschutz

Ein weiterer Kernpunkt im neuen IT-Grundschutz soll die Entwicklung von Profilen werden. Diese sind als Schablonen zu verstehen, mit denen verschiedene Anwender(-gruppen) selbstständig den IT-Grundschutz auf ihre Bedürfnisse anpassen können. Beispielsweise ist es denkbar, dass z. B. mehrere kleine Institutionen, Kommunalverwaltungen, Krankenhäuser und sogar Betreiber kritischer Infrastrukturen zentral definieren, welche Empfehlungen für sie essenziell, optional oder verzichtbar sind.
Bei Bedarf werden während der Projektlaufzeit des Projekts enera geeignete Profile identifiziert und entwickelt. Dies wird im Rahmen von AS 12.2.4 überwacht und bearbeitet.

2.2.3 BDEW Whitepaper

Das BDEW Whitepaper mit dem Titel „Anforderungen an sichere Steuerungs- und Telekommunikationssysteme wurde durch den Bundesverband der Energie- und Wasserwirtschaft (BDEW) in deutscher und englischer Sprache verfasst und später nochmal zusammen mit Österreichs E-Wirtschaft überarbeitet. Es liegt aktuell in der „Version 1.1 03/2015“[18] vor. Das Whitepaper soll Unternehmen dabei unterstützen deren Systeme mit niedrigem oder mittlerem Schutzbedarf vor Sicherheitsbedrohungen im täglichen Betrieb zu schützen, indem festgelegte Sicherheitsmaßnahmen realisiert werden. Bei hohem oder sehr hohem Schutzbedarf muss zusätzlich eine gesonderte Risikoanalyse erfolgen. Weiterhin soll Informationssicherheit bereits in der Planungsphase integriert und insgesamt ein gemeinsames Verständnis in der Branche für Informationssicherheit etabliert werden. Zu dem Whitepaper gibt es ein weiteres Dokument in der Version 1.1 11/2014[19] mit „Ausführungshinweisen zur Anwendung des Whitepaper“ und eine Exceltabelle mit allen Sicherheitsmaßnahmen als Anwendungshilfe. Zusammen können diese als Management-/Monitoring-Tool für die Einhaltung und Entwicklung der Sicherheitsmaßnahmen verwendet werden.

2.2.4 IEC 62351

Die technische Norm IEC 62351 mit dem ins Deutsche übersetzten Titel „Netzführungssysteme und ihr Informationsaustausch - IT Sicherheit“, beschäftigt sich mit IT-Sicherheit und besonders mit Ende-zu-Ende-Sicherheit für Netzführungssysteme. Dieser Standard hat das Ziel eine sichere Kommunikation von Kontrollsystemen im Umfeld der Energiesystemauto-

[18] Das BDEW-Whitepaper kann unter https://www.bdew.de/internet.nsf/id/232E01B4E0C52139C1257A5D00429968/$file/OE-BDEW-Whitepaper_Secure_Systems%20V1.1%202015.pdf abgerufen werden.
[19] Das Dokument „Ausführungshinweise zu Anwendung des Whitepaper“ ist unter https://www.bdew.de/internet.nsf/id/232E01B4E0C52139C1257A5D00429968/$file/OE-BDEW-Whitepaper_Ausf%C3%BChrungshinweise%20V1.1%202015.pdf zu finden.

mation zu definieren. Die IEC 62351 wird von der internationalen Arbeitsgruppe 15 des Technischen Komitees 57 (TC57 WG15) erarbeitet und ist ein Querschnittsstandard zur Informationssicherheit, der sich über alle Ebenen der SIA[20] (Seamless Integration Architecture) erstreckt. Er übernimmt die Spezifikation von Sicherheitserweiterungen für die im TC57 entwickelten Kommunikationsprotokolle. In Abbildung 4 sind die einzelnen Teile des Standards, in Gelb dargestellt, und deren Abhängigkeiten untereinander sowie zu den entsprechenden Kommunikationsstandards, in Grün dargestellt, zu erkennen.

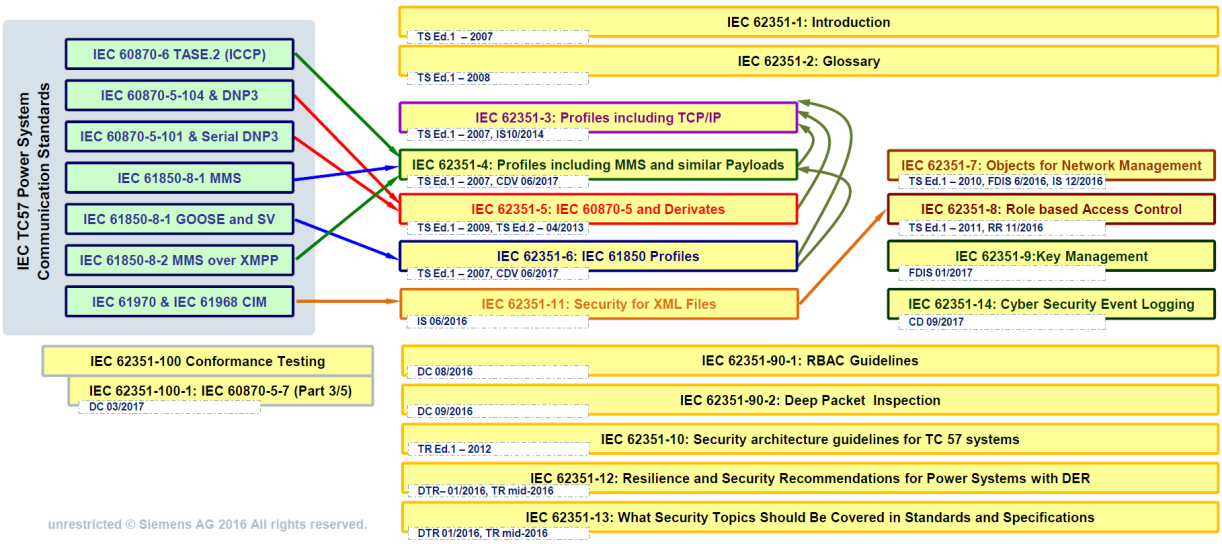


Abbildung 4: Darstellung der Korrelationen zwischen dem IEC 62351 und den verschiedenen Profilen (Quelle: Steffen Fries, Siemens)

Im Folgenden eine kurze Aufzählung der einzelnen Teile der IEC 62351-Standardserie, einzelne Teile sind noch nicht finalisiert oder befinden sich in der Überarbeitung.

- IEC 62351-1, -2: Teil 1 gibt eine Einführung zum Thema und Teil 2 ein Glossar.
- IEC 62351-3, -4, -5 und -6: Teil 3 bis 6 beschreiben Informationssicherheit für verschiedene Profile. Teil 3 für die Internetprotokollfamilie TCP/IP, Teil 4 für MMS-basierte Protokolle, Teil 5 für IEC 60870-5 basierte Protokolle und Teil 6 für IEC 61850 basierte Protokolle.
- IEC 62351-7: Teil 7 behandelt Informationssicherheit für NSM21-Datenobjektmodelle.
- IEC 62351-8: Teil 8 beschreibt eine rollenbasierte Zugriffskontrolle (RBAC) für Leitsysteme.
- IEC 62351-9: Teil 9 erläutert das Schlüsselmanagement im Smart Grid.
- IEC 62351-90-1: Teil -90-1 gibt einen Leitfaden, wie RBAC angewendet werden kann, insbesondere verbraucherbasierte Rollen.
- IEC 62351-90-2: Teil 90-2 beschreibt einen Leitfaden, wie Deep packet inspection bei verschlüsselter Kommunikation ermöglicht werden kann.

[20] Die SIA ist eine Referenzarchitektur notwendiger Standards für die Umsetzung eines Smart Grids und wird im Standard IEC 62357 definiert.
[21] NSM steht für Netzwerk- und Systemmanagement.

- IEC 62351-10: Teil 10 ist eine Richtlinie für Sicherheitsarchitekturen.
- IEC 62351-11: Teil 11 beschäftigt sich mit Informationssicherheit für XML-Dateien.
- IEC 62351-12: Teil 12 gibt Empfehlungen für Ausfall- und Informationssicherheit zwischen dezentralen Energieressourcen (DER).
- IEC 62351-13: Teil 13 ist eine Richtlinie für die Abdeckung von Sicherheitsthemen durch Standards und Spezifikationen im Stromsektor.
- IEC 62351-14: Teil 14 definiert das Event Logging für Cyber Security für Fehleranalysen und Auditing.
- IEC 62351-100, -100-1: Teil 100 dient als Mantel/Schirmstandard dazu Entwicklern zu helfen standardkonforme Funktionalitäten anzubieten. Aktuell sind bisher in Teil 100-1 Testfälle für den Teil 5 des IEC 62351 definiert.

2.2.5 IEC 62443

Der IEC 62443 ist eine Informationssicherheitsstandardreihe für die Automatisierungsindustrie mit dem Titel „Industrielle Kommunikationsnetze - IT-Sicherheit für Netze und Systeme“. Diese Reihe unterteilt sich in vier Themen: allgemeine Vorgaben, Regelwerke und Vorgehensweisen, Vorgaben für das Gesamtsystem sowie Vorgaben für einzelne Komponenten (General, Policies and procedures, System, Component). Diese Themen unterteilen sich in weitere Standardteile, wie in Abbildung 5 dargestellt ist.

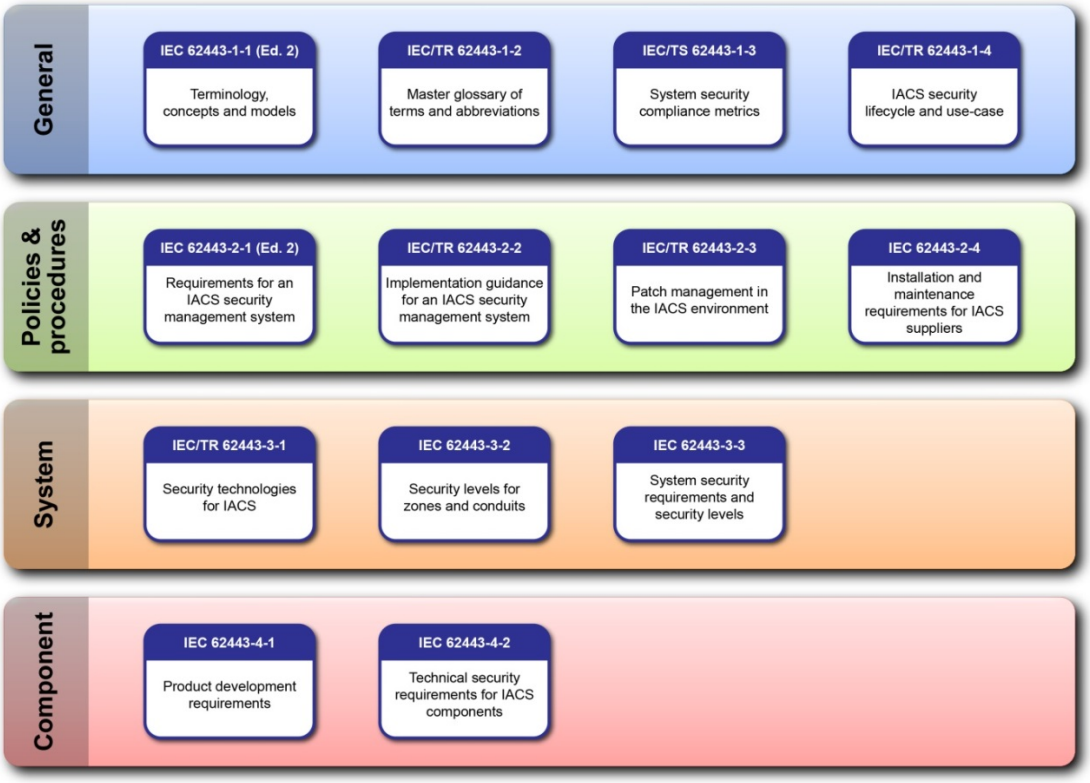


Abbildung 5: Übersicht Normenreihe IEC 62443 (Quelle: www.dke.de)

2.2.6 NISTIR 7628[22]

Das NIST (National Institute for Standards and Technology) ist eine sogenannte nicht-regulative Bundesbehörde innerhalb des US-Wirtschaftsministeriums. Das IR steht für Inter-agency Report beziehungsweise Internal Report.[23] Als Ergänzung zu der Roadmap für das Smart Grid wurde die NISTIR 7628-Richtlinien entwickelt, die einen Leitfaden für Informationssicherheit im Rahmen des Smart Grid beschreiben. Diese Richtlinien beginnen mit einer allgemeinen Einführung in die Thematik, die außerdem die Entwicklungsmethodik der Richtlinien beschreibt. Danach unterteilen sie sich in die folgenden drei Hauptdokumente:
Volume 1 mit dem Titel „Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements“ beschreibt die genutzte Methode zur Identifikation von High-Level Security Anforderungen. Es werden Informationen zum Smart Grid und zu Cyber Sicherheitsstrategien vorgestellt. Das Ziel ist es, die Zuverlässigkeit des Netzes und die Vertraulichkeit von sensiblen Daten zu gewährleisten. Ein High-Level Diagramm wird vorgestellt. Es dient dazu, die Akteure in den Domänen zu verorten. Darauf aufbauend entsteht ein übergreifendes Referenzmodell. Durch dieses werden 22 logische Interface-Kategorien – innerhalb und übergreifend über sieben Smart Grid Domänen – identifiziert und definiert. Daraus werden die sogenannte Smart Grid Cyber Security Requirements abgeleitet. Volume 2 mit dem Titel „Privacy and the Smart Grid“ betrachtet verschiedene Arten des Datenschutzes. Volume 3 mit dem Titel „Supportive Analyses and References“ beschreibt potenzielle Schwachstellen aus verschiedenen Bereichen des Smart Grids.

2.2.7 NERC CIP

Das NERC ist eine Non-Profit-Organisation und ist für die nordamerikanischen Stromnetze zuständig. Die Abkürzung CIP in NERC CIP steht dabei für „Critical Infrastructure Protection“ und bietet standardisierte Handlungsempfehlungen in zehn Teilen (CIP-002 bis CIP-011) für die Zuverlässigkeit des amerikanischen Stromversorgungssystems aktuell in der fünften Revision. Es werden beispielsweise Hinweise für das Training von Personal oder für das Wartungs- und Änderungsmanagement gegeben[24].

2.2.8 ENISA: Appropriate security measures for smart grids[25]

ENISA steht für “European Network and Information Security Agency” (deutsch: Europäische Agentur für Netz und Informationssicherheit) und wurde von der Europäische Union gegründet, um Netz- und Informationssicherheit in der EU zu etablieren und zu verbessern. Diese Agentur hilft den EU-Mitgliedern in Sicherheitsfragen und unterstützt diese, indem Vorgaben und Empfehlungen in Bezug auf Netz- und Informationssicherheit durch die ENISA entwi-

---

[22] Die NISTIR 7628-Richtlinie kann unter http://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.7628r1.pdf abgerufen werden.
[23] Siehe auch http://csrc.nist.gov/publications/PubsNISTIRs.html.
[24] Eine genauere Erläuterung beziehungsweise eine Zusammenfassung der Version 5 dieser Standards ist unter http://www.velaw.com/uploadedfiles/vesite/resources/summarycipversion5standards2014.pdf zu finden. Die jeweilige aktuelle Version der einzelnen Standards ist auf der Homepage des NERC unter http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx abgelegt.
[25] Das Dokument kann unter https://www.enisa.europa.eu/publications/appropriate-security-measures-for-smart-grids/at_download/fullReport abgerufen werden.

ckelt werden. Ein Dokument mit dem Titel „Appropriate security measures for smart grids – Guidelines to assess the sophistication of security measures implementation“ wurde zu Sicherheitsmaßnahmen für das Smart Grid herausgegeben. Dabei vergleicht und bezieht sich die ENISA auf Sicherheitsmaßnahmen bereits bestehender Informationssicherheitsstandards, die teilweise auch in diesem Dokument beschrieben werden, und identifiziert Sicherheitsmaßnahmen für zehn Domänen. Die hier untersuchten Sicherheitsstandards sind Folgende: NISTIR 7628, ISO/IEC 27002, (ISO/IEC DIS 27036-2), (ISO/IEC 27011), NERC CIP, IEC 62443, IEC 62351, ISO/IEC TR 27019, BDEW Whitepaper. Weiterhin werden unterschiedliche Reifegrade (sophistication level) von 1 bis 3 für jede Sicherheitsmaßnahme der zehn Domänen anhand unterschiedlicher Fortschrittsgrade der Sicherheitsrealisierung festgelegt. Dieses Dokument kann somit dafür genutzt werden, Reifegrade für die umgesetzte Informationssicherheit zu bestimmen und anschließend zu identifizieren, welche Maßnahmen ergriffen werden müssen, um die umgesetzte Informationssicherheit zu optimieren.

2.2.9 BSI TR-03109[26]

Die Technische Richtlinie (TR) BSI TR-03109 des BSI definiert die Anforderungen an die Funktionalität, Interoperabilität und Sicherheit, die die Einzelkomponenten in einem Smart Metering System erfüllen müssen, sowie die Anforderungen zur Prüfung dieser Eigenschaften. Sie besteht aus den Teilen TR-03109-1 bis TR-03109-6 sowie Testspezifikationen und Anlagen.

2.2.9.1 BSI TR-03109-1

Teil 1 der Technischen Richtlinie TR-03109 beinhaltet die funktionalen Anforderungen, die ein Smart-Meter-Gateway (SMGW) mindestens erfüllen muss. Das Dokument ist in die drei Themenbereiche Local Meteorological Network (LMN), Home Area Network (HAN) und Wide Area Network (WAN) untergliedert und definiert für diese Bereiche detaillierte technische Vorgaben. Darüber hinaus werden interne, logische Abläufe (bspw. die Tarifierung anhand von Regelwerken, Zusammenspiel zwischen Gateway und Sicherheitsmodul) weiter ausgeführt.

2.2.9.2 BSI TR-03109-2

In Teil 2 der Technischen Richtlinie TR-03109 werden die Anforderungen an die Funktionalität und Interoperabilität des Sicherheitsmoduls für das SMGW spezifiziert. Sie enthält neben einer detaillierten Beschreibung des Lebenszyklus-Modells von Sicherheitsmodul bzw. SMGW insbesondere die Spezifikation des File- und Objektsystems, der Zugriffsregeln und des Kommandosets des Sicherheitsmoduls. In einem Anhang zu dieser Technischen Richtlinie [TR-03109-2A] werden weitere Anwendungsfälle (Use Cases) mit einer Beschreibung der Nutzung des Sicherheitsmoduls durch das SMGW aufgeführt.

2.2.9.3 BSI TR-03109-3

[26] Informationen des BSI zum Schutzprofil des Smart Meter Gateways sowie den dazugehörigen Technischen Richtlinien TR-03109 können unter https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/SmartMeter/SmartMeterGateway/Schutzprofil_Gateway/schutzprofil_smartmetergateway_node.html abgerufen werden.

Das Dokument enthält den Verweis, dass Vorgaben für die verbindlich einzusetzenden kryptographischen Verfahren und Primitive sowie die zu verwendenden Schlüssellängen in der jeweils aktuellen Fassung der BSI TR-03116, Teil 3 „Kryptographische Vorgaben für Projekte der Bundesregierung – Intelligente Messsysteme“ zu finden sind.

2.2.9.4 BSI TR-03109-4

In der TR-03109-4 wird die Architektur der Smart Metering - Public Key Infrastruktur (SM-PKI) spezifiziert, mit der die Authentizität der bei der Kommunikation eingesetzten öffentlichen Schlüssel der Kommunikationspartner auf WAN-Ebene sichergestellt wird. Technisch wird der Authentizitätsnachweis der Schlüssel über digitale Zertifikate aus der SM-PKI realisiert.
Die TR enthält auch die Mindestanforderungen an die Interoperabilität und die Sicherheit der SM-PKI, die in der Zertifizierungsrichtlinie (Certificate Policy, CP) für die SM-PKI berücksichtigt werden müssen. Es werden für die einzusetzenden Zertifikate und Sperrlisten Profile vorgegeben. Ferner werden Protokolle für die Beantragung und Zustellung von Zertifikaten und ein Verzeichnisdienst zur Veröffentlichung der ausgestellten Zertifikate spezifiziert.

2.2.9.5 BSI TR-03109-5

Die „Technische Richtlinie Kommunikationsadapter“ befindet sich aktuell noch in Vorbereitung.

2.2.9.6 BSI TR-03109-6

Der Teil 6 der TR-03109 stellt normative Mindestanforderungen an die Informationssicherheit eines SMGW Admin. Diese Mindestanforderungen sind jeweils durch ein Informationssicherheitsmanagementsystem (ISMS) des SMGW Administrators zu behandeln und konkret auszugestalten. Die Prüfung der Ausgestaltung ist in einem Auditierungsschema geregelt.

Es werden zunächst die Aufgaben und Anwendungsfälle des SMGW Admin beschrieben. Diese leiten sich im Wesentlichen aus dem Gesetz über den Messstellenbetrieb und die Datenkommunikation in intelligenten Energienetzen (Messstellenbetriebsgesetz – MsbG) – Entwurf und BSI TR-03109-1 ab und werden in übersichtlicher Form zusammengefasst.

Das zentrale Kapitel 4 definiert die Sicherheitsanforderungen an den Betrieb des SMGW Admins im Sinne der Informationssicherheit. Dazu wird zunächst auf Schutzziele und zu berücksichtigende Bedrohungen eingegangen. Mindestvorgaben („Mindest-Maßnahmen“) zur Informationssicherheit werden für folgende Bereiche gestellt:

- Dokumentation von Prozessabläufen und Verantwortlichkeiten
- Sensibilisierung der Mitarbeiter
- Inferenzprävention
- Rollen- und Rechtekonzept
- Regelungen zur Vorhaltezeit und Aufbewahrungsdauer von Daten
- SMGW Admin Software und Frontend SMGW Admin Software
- Regelungen für Wartungs- und Reparaturarbeiten

- Entwicklung und Umsetzung eines Anbindungskonzeptes
- Einsatz Zeitserver mit gesetzlicher Zeit
- Netzsegmentierung und -trennung
- Integritätsschutz von IT-Systemen und IT-Komponenten
- Dienstsegmentierung
- Einsatz eines oder mehrerer Protokollierungsserver
- Penetrationstest
- Reaktion auf Verletzung der Sicherheitsvorgaben
- Aufrechterhaltung der Informationssicherheit
- Regelungen für den Einsatz von Fremdpersonal
- Schlüsselmanagement
- SMGW Firmware Update
- Notfallkonzept

Bei der Umsetzung der Anforderungen sind zwei Alternativen möglich: Zum einen die Vorgehensweise und Zertifizierung nach ISO 27001 auf Basis von IT-Grundschutz oder zum anderen die Vorgehensweise nach ISO 27001. Unabhängig von der gewählten Vorgehensweise sind in jedem Fall die Mindestanforderungen zu berücksichtigen und im Rahmen der jeweiligen Sicherheitskonzeption zu betrachten.
Abschließend werden in dem Dokument Rahmenbedingungen für die Auditierung und Zertifizierung aufgezeigt, mit denen die konzipierten Maßnahmen nachweislich geprüft und zertifiziert werden können.

2.2.10 BSI TR-03116-3

Die BSI TR-03109-3 verweist auf diesen Teil 3 der BSI TR-03116 mit dem Titel „Kryptographische Vorgaben für Projekte der Bundesregierung – Intelligente Messsysteme“ (BSI TR-03116-3). In ihm werden die Sicherheitsanforderungen für den Einsatz kryptographischer Verfahren in die Infrastruktur intelligenter Messsysteme im Energiesektor beschrieben. Im Einzelnen werden Anforderungen in folgenden Bereichen formuliert:

- Kryptografische Verfahren und Parameter
- TLS-Kommunikation im Weitverkehrsnetz (WAN)
- TLS-Kommunikation im Home Area Network (HAN)
- TLS-Kommunikation im lokalen metrologischen Netz (Local Metrological Network, LMN)
- Kommunikation im LMN auf Basis symmetrischer Kryptographie
- Inhaltsdatenverschlüsselung und -signatur
- PACE-Protokolle (Password Authenticated Connection Establishment) und Secure Messaging zur sicheren Kommunikation über einen verschlüsselten, authentisierten Kanal zwischen den Smart Meter Gateway und Sicherheitsmodul
- Zertifizierung von Smart Meter Gateways und Sicherheitsmodule nach den Common Criteria

2.2.11 BSI TR-03145

Die Technische Richtlinie BSI TR-03145 „Secure Certification Authority Operation“ wurde vom Bundesamt für Sicherheit in der Informationstechnik (BSI) herausgegeben. Sie formuliert Anforderungen an eine Certification Authority (CA) in einer Public-Key-Infrastruktur (PKI). Die Anforderungen („requirements“ in der englischsprachigen TR) leiten sich aus Funktionalitäten der CA und darauf wirkende Bedrohungen her. Die Anforderungen müssen durch entsprechende Maßnahmen umgesetzt werden. Sie sind als eine Ergänzung zu einem ebenfalls geforderten Informationssicherheitsmanagementsystem (ISMS) nach der internationalen Norm ISO/IEC 27001 oder nach ISO 27001 auf Basis IT-Grundschutz zu verstehen.
Die Umsetzung der Richtlinie kann als „sektor-spezifische Zertifizierung“ zusammen mit der Etablierung des ISMS durch ein Zertifikat des BSI nachgewiesen werden. Das Zertifikat für den ISMS-Anteil kann auch auf Basis ISO 27001 von einer anderen dafür autorisierten Zertifizierungsstelle ausgestellt werden.

Die BSI TR-03145 ist klar strukturiert. Für die einzelnen Prozesse, Aufgaben und Funktionen einer CA sind zunächst die Ziele aufgeführt, gefolgt von Bedrohungen und Sicherheitsanforderungen sowie einer Gegenüberstellung und Begründung, wie den Bedrohungen durch Umsetzung der Anforderungen wirksam begegnet wird. Nach diesem Schema werden folgende Bereiche behandelt:

- Privater Schlüssel der CA
- Verbreitung der Geschäfts und Nutzungsbedingungen und Regeln
- Identifizierung und Registrierung
- Verwaltung der Teilnehmerschlüssel
- Zertifikaterzeugung
- Verbreitung vertrauenswürdiger Zertifikate (public keys)
- Widerruf und Suspendierung von Zertifikaten und Suspendierung von Teilnehmern
- Zertifikatserneuerung, Rekeying und update

Darüber hinaus werden für folgende Bereiche generelle Sicherheitsanforderungen gestellt:

- ISMS
- Zertifikats-Policy und Zertifikats-Practice Statement
- Notfallmanagement und Behandlung von Sicherheitsvorfällen
- Prozessorganisation einschließlich nicht-digitaler Prozesse
- Kryptographische Maßnahmen
- Gesicherter Umgang und Speicherung von Schlüsseln
- Management von Rollen
- Vertrauenswürdiges Personal
- Gehärtete IT-Systeme und Netze mit Unterstützung von Logging und Monitoring
- Archivierung und Nachverfolgung
- Sichere Pflege und Verwaltung des Widerruf-Status
- Physische und umgebungsbezogene Sicherheit
- Verfügbarkeit von Diensten
- Sichere Beendigung einer CA

- Anforderungen an Unterauftragnehmer

2.2.12 Common Criteria (ISO/IEC 15408)

Die Common Criteria for Information Technology Security Evaluation (Common Criteria, CC; deutsch: Allgemeine Kriterien für die Bewertung der Sicherheit von Informationstechnologie) sind ein internationaler Standard zur Prüfung und Bewertung der Sicherheitseigenschaften von IT-Produkten.
Die Version 3.1 wurde 2006 im internationalen Common Criteria Anerkennungsabkommen verabschiedet und gemäß BSI-Zertifizierungsverordnung im Bundesanzeiger vom 23.02.2007 offiziell bekannt gegeben. Diese Version der CC liegt ebenfalls als internationaler Standard ISO/IEC 15408 vor. Ebenso verabschiedet wurde die gemeinsame Evaluationsmethodologie (Common Methodology for Information Security Evaluation CEM) Version 3.1 welche eine abgestimmten Methodik für die Evaluierung auf Grundlage der CC festlegt und auch als internationaler Standard ISO/IEC 18045 vorliegt.
Die CC umfassen drei Teile:

- Teil 1: Hier werden „Einführung und allgemeines Modell / Introduction and General Model“ die Grundlagen der IT-Sicherheitsevaluation und der allgemeine Geltungsbereich der CC erläutert. In den Anhängen werden Schutzprofile (Protection Profile) und Sicherheitsvorgaben (Security Target) für den zu prüfenden Evaluationsgegenstand (EVG) beschrieben.
- Teil 2: „Funktionale Sicherheitsanforderungen / Functional Requirements“ enthält Funktionalitätsanforderungen in Form eines Kataloges, welcher Empfehlungen (d.h. keine zwingenden Vorgaben) für die Beschreibung der Funktionalität eines Evaluationsgegenstandes macht. Die Zusammenhänge von Bedrohungen, Sicherheitszielen und funktionalen Anforderungen sind im Anhang erläutert.
- Teil 3: Hier werden „Anforderungen an die Vertrauenswürdigkeit / Assurance Requirements“ die Anforderungen an die Vertrauenswürdigkeit dargestellt.

Grundgedanke der CC ist die Unterscheidung zwischen der **Funktionalität** (Funktionsumfang) eines Systems und der **Vertrauenswürdigkeit** (Qualität).
Funktionale Sicherheitsanforderungen werden in Klassen zusammengefasst. Beispiele für wichtige Klassen sind:

- FAU Security Audit (Sicherheitsprotokollierung)
- FCO Communication (Kommunikation)
- FCS Cryptographic Support (Kryptographische Unterstützung)
- FDP User Data Protection (Schutz der Benutzerdaten)
- FIA Identification and Authentication (Identifikation und Authentisierung)
- FMT Security Management (Sicherheitsmanagement)
- FPR Privacy (Privatheit)
- FPT Protection of the TSF (Schutz der Sicherheitsfunktionen)
- FRU Ressource Utilisation (Betriebsmittelnutzung)
- FTA Target of Evaluation Access (Schnittstelle)

- FTP Trusted Path/Channels (Vertrauenswürdiger Pfad/Kanal)

Für die **Vertrauenswürdigkeit** sind sieben Abstufungen vorgesehen (Evaluation Assurance Level, EAL1-7). Sie spiegeln die Korrektheit der Implementierung des betrachteten Systems bzw. die Prüftiefe mit der dies nachgewiesen wurde wieder. Es sind:

- EAL1: funktionell getestet
- EAL2: strukturell getestet
- EAL3: methodisch getestet und überprüft
- EAL4: methodisch entwickelt, getestet und durchgesehen
- EAL5: semiformal entworfen und getestet
- EAL6: semiformal verifizierter Entwurf und getestet
- EAL7: formal verifizierter Entwurf und getestet

Anforderungen an die Funktionalität sowie an die Vertrauenswürdigkeit werden in **Schutzprofilen** zusammengefasst und decken eine bestimmte Menge von Sicherheitszielen vollständig ab. Es werden generische Anforderungen an eine Produktkategorie festgeschrieben, welche zunächst implementierungsunabhängig sind, und durch die daraus ableitbaren Sicherheitsvorgaben auf einen konkreten Evaluationsgegenstand (EVG) zugeschnitten werden können.

Beispiele für Schutzprofile des BSI sind:

- BSI-CC-PP-0073-2014 beschreibt die Anforderungen an ein Gateway, welches die zentrale Kommunikationseinheit für ein intelligentes Messsystem darstellt. Das Gateway stellt zentrale Funktionen zum sicheren Abruf, Speicherung, Aufbereitung und Versendung von Messdaten von einem oder mehreren Mandanten bereit.
- BSI-CC-PP-0077-V2-2015 beschreibt die Anforderungen an ein Sicherheitsmodul, das für den Einsatz in einem Smart-Meter-Gateway vorgesehen ist. Das Sicherheitsmodul stellt zentrale kryptografische Funktionen zur Verfügung, sowie das sichere Speichern kryptografischer Schlüssel und weiterer Daten, die für das Gateway relevant sind.

2.2.13 Zusammenfassung „Normen, Standards und Richtlinien“

Die folgende Tabelle 6 gibt einen Überblick über die in diesem Abschnitt 2.2 beschriebenen Normen, Standards und Richtlinien. Die Kategorien in den sind dabei angelehnt an die „Smart Energy Grid – Coordination Group“ von CEN-CENELEC-ETSI in ihrem „Cyber Security and Privacy“-Bericht.

Standard	Sprache		Ursprüngliche Domäne			Art der Vorgaben			Adressat		
	deutsch	englisch	Informationssysteme	Energieversorgung	Industrielle Automatisierung	Richtlinien	Anforderungen	Umsetzung	Betreiber	Systemintegrator	Entwickler
ISO/IEC 27001/02	x	x	x				x		x		
ISO/IEC TR 27019				x			x	x	x		
BSI Grundschutz	x		x					x		x	
BDEW Whitepaper	x	x		x			x		x	x	x
IEC 62351		x		x		x		x	x	x	x
IEC 62443		x			x		x	x	x	x	x
NISTIR 7628		x		x			x			x	x
NERC CIP		x		x			x	x	x		
ENISA „Smart Grid“		x		x		x			x	x	x
BSI TR-03109	x			x				x	x		x
BSI TR-03116-3	x			x				x			x
Common Criteria		x	x				x				x
BSI TR-03145		x	x					x			x

Tabelle 6: Übersichtstabelle Normen, Standards und Richtlinien

Die folgende Tabelle 7 ordnet die hier beschriebenen Normen, Standards und Richtlinien den einzelnen Arbeitspaketen (APs) aus enera zu. Dabei ist jeder AP-Nummer ein Kurztitel zur besseren Verständlichkeit angehängt. Diese Zuordnung zu den APs erfolgte im Rahmen von AS 12.2.1 und soll durch die Schnittstellenverantwortlichen für Informationssicherheit in den APs überprüft werden. Ein „x“ pro Zelle bedeutet dabei, dass das entsprechende Gesetz eine Relevanz für das AP aufweist. Ein „(x)“ pro Zelle heißt, dass das entsprechende Gesetz eine Relevanz für das AP ausweisen kann bzw. es gibt eine indirekte Relevanz des Gesetzes für das AP.

AP-Nummer – Kurztitel	ISO/IEC 2700x	BSI Grundschutz	BDEW Whitepaper	IEC 62351	IEC 62443	NISTIR 7628	NERC CIP	ENISA	TR-03109	BSI TR-03116	Common Criteria	TR-03145
AP1 – Digitale Konnektivität	x	x	x			x		x	x	x	x	x
AP2 – SDSP	x	(x)		(x)	(x)	(x)		x	(x)			
AP3 – SG-Operator	x	x	x	x		x	x	x	x	x	x	
AP4 – Rollout Netzbetriebsmittel	x	x	x	x		x	x	x				
AP5 – Flexibilisierung	x	x	x			x		x				
AP6 – Technische Entwicklung regionaler Produkte	x	x	x			x		x				
AP7 – Marktintegration regionaler Produkte	x	x										
AP8 – Energierecht												
AP9 – Neue Geschäftsmodelle	x	x										
AP10 – enera Qualifizierungscenter												
AP11 – Bürgerbeteiligung	x	x										
AP12 – Architektur und Security	x	x	x	x	x	x	x	x	x	x	x	x
AP13 – Nationaler/Internat. Transfer	x			x			x	x				
AP14 – Projektmanagement												

Tabelle 7: Relevanz der Normen, Standards und Richtlinien für die einzelnen APs aus enera

2.3 Informationssicherheit in der Software Entwicklung

Grundsätzlich orientiert sich der Bedarf an Sicherheit einer Software-Lösung an den Anforderungen der Domäne, in denen die Software zum Einsatz kommt bzw. kommen soll. Allgemeingültige und übergreifende Anforderungen an die Sicherheit von Software sind daher nicht vorhanden. Unabhängig von expliziten Anforderungen besteht beim Einsatz von Software jedoch bei allen Anwendern der grundlegende Bedarf, dass diese sicher ist und wie erwartet zur Verfügung steht. Außerdem muss es sich um wirtschaftlich angemessene Sicherheitslösungen handeln.

Bei der Entwicklung von Software-Lösungen sind daher die Anforderungen an die Sicherheit(sfunktionen) der Software vorab zu klären (Anforderungsmanagement). Diese Anforderungen sind anschließend im Rahmen der Softwareentwicklung zu berücksichtigen sowie umzusetzen. Vor Abschluss der Entwicklungstätigkeiten sind die implementierten Sicherheitsfunktionen innerhalb des Testmanagements zu überprüfen. Hierbei sollten zusätzliche Testfälle definiert werden, welche nicht nur die Funktionsfähigkeit sicherstellen, sondern auch die Robustheit (Verhalten im Fehlerfall). Alle Tätigkeiten werden in der Regel über die Verfahren zur Softwareentwicklung koordiniert, welche nachfolgend kurz erläutert werden.

2.3.1 Klassische Verfahren Softwareentwicklung

2.3.1.1 V-Modell

Das V-Modell wird als ein generalisierter Rohling deklariert, welcher auf ein konkretes Projekt angepasst werden kann. Anders als bei sonstigen klassischen Modellen werden im V-Modell **Aktivitäten** und **Ergebnisse** definiert. Auf eine zeitlich strikte Abfolge wird dabei verzichtet. Darüber hinaus fehlen die typischen Abnahmen, welche Phasenenden definieren. Dennoch ist es möglich, die Aktivitäten des V-Modells zum Beispiel auf ein Wasserfallmodell abzubilden. Die Grundelemente des V-Modells bilden folgende Komponenten:

- Aktivitäten: Tätigkeiten im Software-Entwicklungsprozess
- Ergebnisse: Artefakte der Aktivitäten

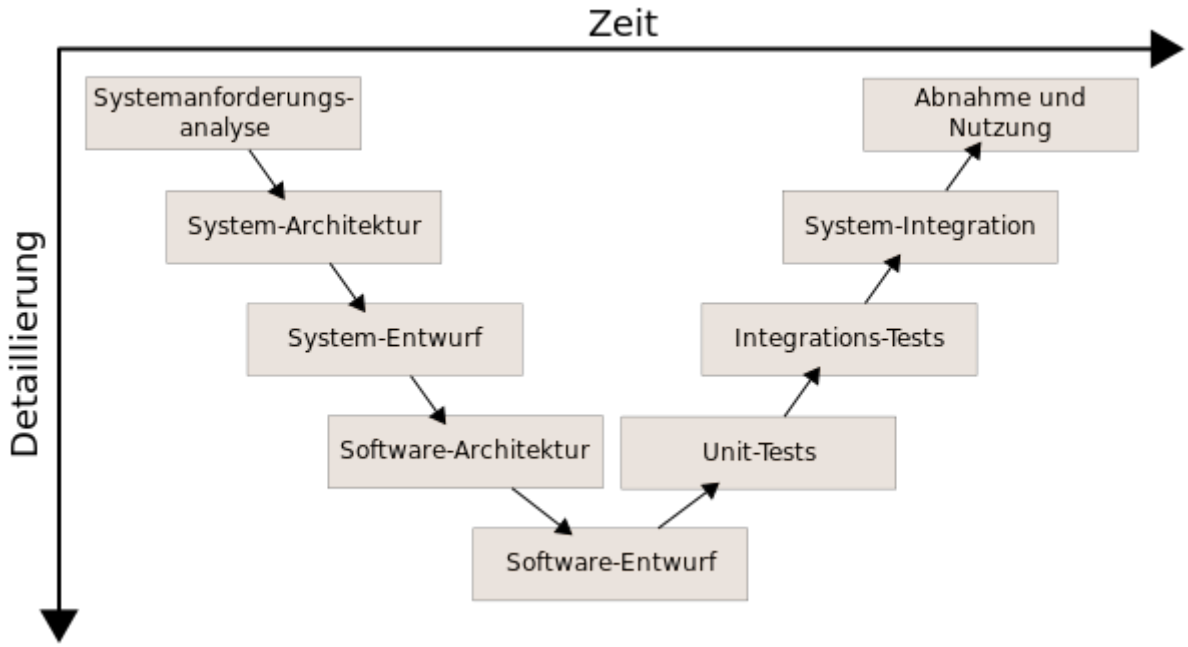


Abbildung 6: Schema des V-Modells (Quelle: Michael Pätzold, S. Seyfert)

Das V-Modell wird immer in folgende Sub-Modelle untergliedert. Nicht benötigte Aktivitäten und Ergebnisse werden nach Bedarf herausgenommen, dies ist das sogenannte „Tayloring“.

- Software-Erstellung
- Qualitätssicherung
- Konfigurationsmanagement und
- Projektmanagement

2.3.1.2 Wasserfallmodell

Das Wasserfallmodell setzt sich aus folgenden Schritten zusammen:

- Aufstellen der Anforderungen
- Systemanalyse
- Systementwurf
- Implementierung
- Test und Integration

- Abnahme

Jeder dieser Schritte wird im Wasserfallmodell als genau eine Phase abgebildet. Daher handelt es sich bei einem Wasserfallmodell um ein Phasenmodell. Jede Phase hat eine definierte Aufgabenstellung, die zu einem definierten Phasenergebnis führen soll.
Das Ergebnis einer Phase stellt die Eingabe und den Start der nächsten Phase dar. Wenn die vorherige Phase mit einer Qualitätsprüfung freigegeben und abgeschlossen wurde, kann die nächste Phase begonnen werden. Bei entdeckten Fehlern oder Änderungswünschen während der Qualitätsprüfung, kann die nächste Phase nicht angestoßen werden. Erst die Freigabe – aufgrund einer ausreichenden Qualität – durch einen Verantwortlichen, führt zum Sprung in die nächste Phase. Werden an den Phasengrenzen der sequentiellen Entwicklungsschritte Qualitätsprüfungen durchgeführt, so kann das Wasserfallmodell als Baseline Management-Modell bezeichnet werden.

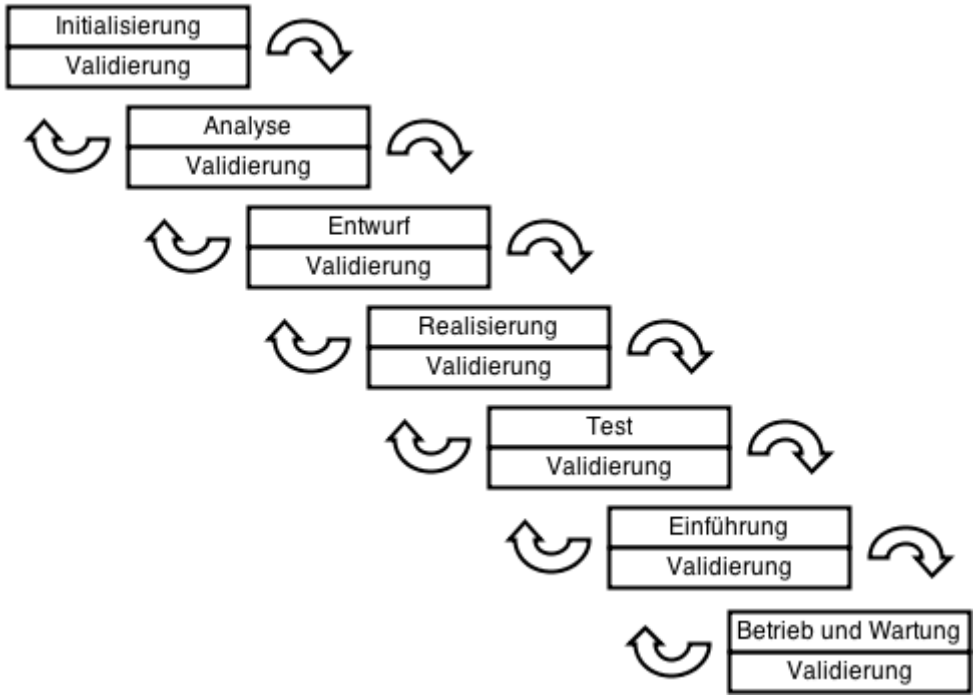


Abbildung 7: Schema des Wasserfallmodells nach Boehm (Quelle: http://winfwiki.wi-fom.de/index.php/Erstellung_einer_Entscheidungsgrundlage_für_die_Einführung_einer_agilen_Softwareentwicklungsmethode#Aktuelles_Vorgehensmodell)

2.3.2 Agile Verfahren Softwareentwicklung

Für Vorgehensweisen in der klassischen Softwareentwicklung wird grundsätzlich der Begriff **Vorgehensmodell** verwendet. In der agilen Softwareentwicklung ist die Verwendung des Begriffs Vorgehensmodell schwierig, da Schwerpunkte vielmehr auf Werte und Praktiken statt auf organisatorische Rahmen gelegt werden. Daher wird in diesem Zusammenhang der Begriff **Methodik** angewendet. Allen Methoden der agilen Softwareentwicklung liegt das Agile Manifest zugrunde. Die jeweiligen Vorgehensweisen und Konzepte basieren auf den dort erwähnten Werten.
Wesentlich für agile Softwareentwicklungen sind möglichst **häufige Rückkopplungsprozesse** und zyklische (iterative) Vorgehensweisen auf allen Ebenen. Mit Ebenen sind hier die Teams, das Management und die Programmierung gemeint. Das neu zu entwickelnde Sys-

tem wird bei der agilen Softwareentwicklung nicht im Vorfeld detailliert geplant und dann in einem einzigen Lauf entwickelt. Bei der Entwicklung wechseln kurze Planungs- und Entwicklungsphasen miteinander ab. Ein Plan für eine erste Version wird dann ausgearbeitet, wenn eine erste Vision, also die Ziele für das System, festgelegt und gewichtet worden sind. Notwendige Anpassungen bezüglich der Entwicklungsgeschwindigkeit, der organisatorischen Rahmenbedingungen und der möglichen Probleme, werden erst nach diesem Schritt durchgeführt. Eine Basisversion mit den wichtigsten Features soll möglichst schnell entwickelt werden, um diese gemeinsam mit dem Kunden zu bewerten, erforderliche Anpassungen vorzunehmen und nachfolgende Versionen besser optimieren zu können.
Um diesen Anforderungen gerecht zu werden, soll der Kunde mit dem Management und den Entwicklern eng zusammenarbeiten und in Standup-Meetings gerade fertiggestellte und zeitnah anfallende Arbeiten kommunizieren. Die von Kunde und Management vorgegebenen Geschäftsziele sollen mit jeder neuen Software in Anforderungen überführt werden, denen das neue System entsprechen soll.
Im Rahmen der agilen Softwareentwicklung bestehen folgende agile Methoden:

- **Scrum**
  Scrum richtet sich eher in Richtung Management aus. Dabei werden grundsätzlich Intervalle von 30 Tagen angelegt, in denen eine bestimmte Anzahl von Anforderungen abgearbeitet werden sollen. Diese Anforderungen wurden im Vorhinein priorisiert (Backlog). Zusätzlich findet jeden Tag ein 15-minütiges Scrum Meeting statt, welches die hauptsächliche Koordination der Beteiligten regelt.
- **Xtreme Programming (XP)**
  XP ist eine der beliebtesten agilen Methoden, die aus den Erfahrungen bei der Entwicklung eines Informationssystems bei Daimler Chrysler entstanden ist und als sehr prinzipientreu gilt. Alle in XP definierten Methoden sollten gemäß Lehrbuch angewendet werden. Praktiken wie User Stories, Pair Programming, Simple Design, Test First und Continuous Integration sind umzusetzen.
- **Adaptive Software Development (ASD)**
  ASD entstand als Reaktion auf Turbolenzen der Industrie und mit dem Wunsch nach schneller Umsetzung von fachlichen Anforderungen. ASD bietet eine philosophische Basis und einen praxisorientierten Ansatz. Dabei spielten iterative Entwicklungsprozesse, Feature-Based Planning und eine Fokussierung auf Kundenanforderungen entscheidende Rollen.
- **Feature-Driven Development (FDD)**
  Ein sehr leichtgewichtiger, architekturbasierter Prozess, welcher zu Beginn eine Gesamtübersicht zur Architektur und Features auflistet. Anschließend werden Methoden wie Design-By-Feature und Build-By-Feature angewendet. Zentrale Rollen sind hierbei der Chef Architekt und der Chef Entwickler. UML und andere Objektorientierte Design Methoden spielen eine zentrale Rolle.

2.3.3 Security-by-Design Prinzipien und Security Patterns

Auch wenn es keine allgemeingültigen Anforderungen an Software-Lösungen gibt, so existieren Grundsätze bzw. Prinzipien, welche bei Berücksichtigung insbesondere kritische Sicher-

heitslücken bei Systemen vermeiden können. Dabei sind diese **Prinzipien** als Ziele zu verstehen, welche im Kontext des jeweiligen Entwicklungsvorhabens auf Anwendbarkeit geprüft sowie entsprechend umgesetzt werden können.

- **Minimierung der Angriffsfläche**
  Jede Funktion, die einer Anwendung hinzugefügt wird, fügt der Gesamtanwendung ein gewisses Risiko hinzu. Ziel der sicheren Entwicklung ist es, das Gesamtrisiko durch eine Verringerung der Angriffsfläche zu reduzieren. Zum Beispiel ist in einer Web-Anwendung eine Online-Hilfe mit einer Suchfunktion vorhanden. Die Suchfunktion kann anfällig für SQL-Injection-Angriffe sein. Wenn die Hilfefunktion auf autorisierte Benutzer beschränkt ist, wird die Angriffswahrscheinlichkeit reduziert.
- **Nutzung sicherer Standardwerte**
  Es gibt viele Möglichkeiten, um eine „out of the box“ Erfahrung für Benutzer zu liefern. Allerdings sollte die Erfahrung standardmäßig sicher sein und es dem Benutzer überlassen werden, die Sicherheit zu reduzieren, wenn dies zulässig ist. Beispielsweise sollten Kennwortgültigkeit und Komplexität standardmäßig aktiviert sein. Benutzer können diese beiden Funktionen ausschalten, um die Nutzung der Anwendung zu vereinfachen, dabei wird gleichzeitig das eigene Risiko erhöht.
- **Prinzip der geringsten Berechtigung**
  Das Prinzip der geringsten Berechtigung empfiehlt, dass Konten die geringste Berechtigung für die Ausführung ihrer Aktivitäten haben. Dies umfasst Benutzerrechte, Ressourcenberechtigungen wie CPU-Grenzwerte, Speicher-, Netzwerk- und Dateisystemberechtigungen. Zum Beispiel, wenn ein Proxy-Server nur Zugriff auf das Netzwerk, lesenden Zugriff auf eine Datenbanktabelle und die Möglichkeit in ein Protokoll zu schreiben erfordert, werden alle erforderlichen Berechtigungen in einer entsprechenden Rolle zusammengefasst. Unter keinen Umständen sollten dem Server Administratorrechte eingeräumt werden.
  Ein Konzept dieses Prinzip umzusetzen ist die rollenbasierte Zugriffskontrolle (engl. role based access control, RBAC). Dabei werden den Nutzern Rollen zugewiesen, so dass sie nur minimale Rechte und somit nur Zugriff haben, um ihre entsprechenden Aufgaben zu erfüllen. Ein Nutzer kann je nach Aufgabentätigkeit mehreren Rollen zugeordnet sein.
- **Prinzip „Defense in depth“**
  Das Prinzip „Defense in depth“ verfolgt, dass dort, wo eine Kontrolle sinnvoll ist, mehrere Kontrollen, die die Risiken in unterschiedlicher Weise vermeiden, besser sind. Denn verschachtelte und tief im System befindliche Kontrollen können außerordentlich schwierig ausgenutzt werden und sind somit unwahrscheinlich als Quellen für schwerwiegende Sicherheitslücken. Dies kann in Form von mehrstufigen Validierungen, zentralisierten Audit-Kontrollen und stetige Prüfung auf autorisierte Benutzer erfolgen.
- **Vollständige Zugriffskontrolle**
  Jeder Objektzugriff muss hinsichtlich seiner Berechtigung geprüft werden. Der Hintergedanke ist hierbei, die Autorisierung nicht nur an einer Stelle durchzuführen und Auswirkungen von Fehlern in der Implementierung so einzuschränken. Beispielsweise sollte nach diesem Prinzip nicht nur der Zugriff auf bestimmte Objekte in der Präsentationsschicht, sondern (sofern möglich) auch auf Datenbankebene geprüft werden.

- **Sichere Fehlerbehandlung und Protokollierung**
  Anwendungen schlagen regelmäßig bei der Abarbeitung von Transaktionen fehl – aus unterschiedlichsten Gründen. Es ist daher stets auf eine sichere Fehlerbehandlung im Rahmen der Anwendung zu achten. Damit Angriffe auf Anwendungen (überhaupt) nachvollzogen werden können, ist es erforderlich, dass die in der Anwendung aufgetretenen Fehler in sicherheitsrelevanten Funktionen (etwa bei der Authentisierung) protokolliert werden.
- **Vertrau keinen IT-Services**
  Viele Organisationen nutzen die Verarbeitungskapazitäten von Dritten, die sehr wahrscheinlich andere Sicherheitsrichtlinien und -vorgaben haben als die Organisation selbst. Es ist unüblich, dass Vorgaben bei Externen von außen beeinflusst oder kontrolliert werden können. Daher ist ein implizites Vertrauen für extern betriebene Systeme nicht gerechtfertigt. Alle externen Systeme sollten in ähnlicher Weise behandelt werden. Zum Beispiel sollten Daten, welche von einem externen System verarbeitet und zurückgespielt werden, vor der Weiterverarbeitung auf Plausibilität überprüft werden.
- **Minimale gemeinsame Ressourcen**
  Der Zugriff auf gemeinsam genutzte Ressourcen, wie beispielsweise globale Variablen, durch mehrere Benutzer oder Prozesse ist weitestgehend zu minimieren. Jede gemeinsam genutzte Ressource enthält mögliche unerwünschte Informationsflüsse. Auch kann dies dazu führen, dass ein Benutzer (oder Prozess) die Ressourcen eines anderen beeinflusst. Wenn möglich sollen gemeinsam genutzte Ressourcen daher sinnvoll separiert werden. Dies kann zum Beispiel durch den Einsatz lokaler Variablen bzw. Virtualisierung geschehen.
- **Trennung von Rollen**
  Ein Schlüssel zum Schutz vor Betrug ist die Trennung von Rollen. Zum Beispiel muss, wenn eine Person (z.B. ein Angestellter) eine Zahlung anweist, eine weitere Person mit einer anderen Rolle (z.B. sein Vorgesetzter) diese Zahlung bestätigen. Bestimmte Rollen haben ein anderes Vertrauenslevel als normale Benutzer. Insbesondere sind Administratoren anders zu handhaben als normale Benutzer. Im Allgemeinen sollten Administratoren nicht auch Benutzer der Anwendung sein. Zum Beispiel sollte ein Administrator in der Lage sein, das System ein- oder auszuschalten oder die Kennwortrichtlinie festzulegen, nicht aber sich am Webportal als hochprivilegierter Benutzer anzumelden, um zum Beispiel Waren im Namen anderer Benutzer zu kaufen.
- **„Keep it simple“**
  Angriffsfläche und Einfachheit gehen Hand in Hand. Neue Vorgehensweisen bevorzugen teilweise übermäßig komplexe Ansätze, die sonst mit relativ einfachen Methoden gelöst werden könnte. Entwickler sollten die Verwendung von doppelten negativen Prüfungen und komplexen Architekturen vermeiden, wenn ein alternativer / klassischer Ansatz schneller und einfacher wäre.
- **Sicherheitsprobleme richtig beheben**
  Sobald ein Sicherheitsproblem identifiziert wurde, ist es wichtig, einen Test für dieses zu entwickeln und die Ursache des Problems zu verstehen. Wenn Design-Muster verwendet werden, ist es wahrscheinlich, dass das Problem in der Anwendung weit verbreitet ist.

Die Entwicklung der richtigen Korrektur ohne Einführung von neuen Schwachstellen ist daher von wesentlicher Bedeutung, um das System vollständig abzusichern.

Weiterhin können **Security Patterns** bei der Berücksichtigung von Sicherheitslösungen in der Softwareentwicklung verwendet werden. Entwurfsmuster bzw. „Software Patterns“ liefern eine abstrahierte Lösung für ein Problem, das in einem spezifischen Kontext auftritt. Sie bieten also auch Lösungen, die unabhängig von der Programmiersprache sind. Neben Entwurfsmustern[27] für eine Architektur gibt es spezielle Entwurfsmuster für den Bereich der Informationssicherheit (Security Patterns). Diese Entwurfsmuster abstrahieren Lösungen für typische Sicherheitsprobleme in bestimmten Kontexten.
Die Dokumentation von Patterns für die Informationssicherheit unterscheidet sich kaum von typischen Software Patterns. Neben einer allgemeinen Beschreibung enthält ein Entwurfsmuster typischerweise den vorgesehenen Kontext und eine abstrakte Problem- sowie Lösungsbeschreibung. Weiterhin sind Informationen wie Implementierungshinweise, Beispiele, bekannte Einsatzgebiete und mögliche Seiteneffekte sinnvolle Ergänzungen.
Entwurfsmuster für Informationssicherheit lassen sich in verschiedene Bereiche einordnen wie Entwurfsmuster für das Risikomanagement, zur Zugriffskontrolle, für Firewall-Architekturen und Entwurfsmuster für sichere Webanwendungen. Nach Schumacher et al.[28] erfolgt die Unterteilung der Security Pattern Landschaft in folgende Kategorien:

- Enterprise Security and Risk Management Patterns
- Identification & Authentication (I&A) Patterns
- Access Control Model Patterns
- System Access Control Architecture Patterns
- Operating System Access Control Patterns
- Accounting Patterns
- Firewall Architecture Patterns
- Secure Internet Applications Patterns
- Cryptographic Key Management Patterns
- Related Security Pattern Repositories Patterns

2.3.4 Best Practices für Software(entwicklung)

Zur Erhöhung der Sicherheit von Software ist es ebenfalls sinnvoll, auf Erfahrungen und erfolgreichen Lösungswegen (Best Practices) von Dritten aufzubauen. Oft lassen sich von den Lösungen Ansätze für die eigenen Entwicklungstätigkeiten ableiten. Hierfür ist es sinnvoll, die in der jeweiligen Technologie führenden Fachgremien bzgl. vorhandener Best Practices zu kontaktieren. Ebenfalls bieten viele Hersteller von Basiskomponenten (wie z. B. einem Betriebssystem oder einer Datenbanklösung) Hinweise und Empfehlungen zur sicheren Verwendung der jeweiligen Technologie.

[27] Siehe z.B. “Design Patterns: Elements of Reusable Object-Oriented Software” von Gamma, Helm, Johnson, Vlissides.
[28] Siehe “Security Patterns - Integrating Security and Systems Engineering” von Schumacher, Fernandez-Buglioni, Hybertson, Buschmann, Sommerlad

Ergänzend gibt es allgemeine Übersichten zu Sicherheitsproblemen, welche häufig zu Sicherheitslücken geführt haben. Hier sei als Beispiel auf das Open Web Application Security Project (OWASP) verwiesen, welches regelmäßig die aktuellen „Top-Bedrohungen“ im Kontext von Web-Applikationen[29] sowie mobilen Applikationen[30] zur Verfügung stellt.
Insgesamt gilt es wiederkehrende Muster von Schwachstellen zu vermeiden[31]: An erster Stelle sind dies **Designfehler**, z.B. die mehrfache Haltung von Benutzerdaten, die besonders geschützt sein sollten, in verschiedenen Datenbanken. Bei Designfehlern besteht meist die Notwendigkeit eines Redesigns. Im Vergleich dazu können Codingfehler meist mit lokalem Patch behoben werden. Es besteht außerdem häufig das Problem **unsicher mit Ein- und Ausgaben umzugehen**, beispielsweise SQL-Injection oder Cross-site Scripting (siehe auch OWASP Top 10). Maßnahmen hierbei sind die Input-Validierung, d.h. die Eingaben genau darauf prüfen, ob sie enthalten, was erwartet wird, also Whitelisting statt Blacklisting zu betreiben. Außerdem sollte Output Sanitisierung verwendet werden, d.h. Ausgaben genau darauf prüfen, ob sie enthalten, was erwartet wird und nur in dem gewünschten Typ (z.B. ein Bild). Auch wenn ein hoher Aufwand nötig ist diese Schwachstelle auszunutzen, ist es wichtig nicht **unsicher im Umgang mit dem Speicher** zu sein und somit z.B. Buffer Overflows zu vermeiden. Man kann dies umgehen, indem man sichere Funktionen und Sprachen verwendet, also keine Programmiersprachen, die Speichermanipulation erlauben bzw. nur Funktionen verwenden, die den Speicherbereich kontrollieren. Weiterhin ist der **unsichere Umgang mit Wettlaufsituationen (race conditions)** ein wiederkehrendes Muster, beispielsweise der gleichzeitige Zugriff auf gemeinsame Informationen. Dies lässt sich verhindern, indem atomare Funktionen verwendet werden. Auch der **unsichere Umgang mit Berechtigungen und Ressourcen** spielt häufig eine Rolle bei den Schwachstellen einer Implementierung. Z.B. der nicht autorisierte Zugriff auf Informationen sollte vermieden werden. Hier sollten minimale Rechte gesetzt werden, z.B. Zugriffe auf die Sichtbarkeit von Ressourcen sollten eingeschränkt sein. Diese Muster von Schwachstellen werden u.a. durch die OWASP Top 10 oder auch die „24 Sins of Software Security“[32] abgedeckt.

2.3.5 Anforderungen an Softwareentwicklung gemäß BSI

Zur Orientierung, welche Aktivitäten im Rahmen der Softwareentwicklung zu berücksichtigen sind, um eine möglichst hohe Sicherheit der Software zu erreichen, hat das BSI einen entsprechenden BSI-Baustein zur Verfügung gestellt. Der Baustein beschäftigt sich mit allen relevanten Aspekten, die von Institutionen bei Entwicklung von Software zu beachten sind. Hierzu werden Vorbereitung, Abwicklung und Inbetriebnahme seitens der Institution betrachtet und dementsprechende Gefährdungen und Maßnahmen ausgewählt. Der Baustein stellt keine vollständige Anleitung zur generellen Vorgehensweise bei der Software-Entwicklung dar, sondern konzentriert sich auf die relevanten Aspekte der Informationssicherheit bei der

[29] https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project
[30] https://www.owasp.org/index.php/OWASP_Mobile_Security_Project#Top_Ten_Mobile_Risks
[31] Siehe Buch “Basiswissen Sichere Software – Aus- und Weiterbildung zum ISSECO Certified Professional for Secure Software Engineering” von Sachar Paulus.
[32] Siehe Buch “24 Deadly Sins of Software Security – Programming Flaws and How to Fix Them“, Michael Howard, David LeBlanc, John Viega, McGrawHill, 2010.

Software-Entwicklung. Nachfolgend werden die Kernaspekte vorgestellt – eine vollständige Einsicht ist auf den Webseiten des BSI[33] möglich.

Hinweis: Wenn nachfolgend eine Bezeichnung im Format „M X.Y“ als Referenz verwendet wird, entspricht X einem der sechs Maßnahmenkateloge und Y der Nummer der entsprechenden Maßnahme aus dem IT-Grundschutz des BSI. Bei der Bezeichnung „B Y.Z“ handelt es sich um einen entsprechenden Baustein aus den BSI IT-Grundschutzkatalogen. Die Kataloge können ebenfalls auf der Webseite des BSI eingesehen werden.

Im Zuge der aktuellen Umstrukturierung des BSI-Grundschutzes werden auch die Bausteine und Maßnahmen überarbeitet (wie schon in Abschnitt 2.2.2 zum BSI Grundschutz erwähnt). Auch der IT-Grundschutz-Katalog-Baustein B 5.27 wird im Rahmen des IT-Grundschutz-Katalog-Bausteins „CON – Konzepte und Vorgehensweisen“ überarbeitet. Spätestens im Oktober 2017 soll der IT-Grundschutz-Katalog-Baustein CON.3 zum Thema Softwareentwicklung veröffentlicht werden.

In der folgenden Aufzählung wird das Vorgehen innerhalb des für diese Thematik relevanten Bausteins „B 5.27 Software-Entwicklung“ kurz beschrieben.

- **Planung und Konzeption**
  Eine sorgfältige Planung und Konzeption ist essenziell bei der Entwicklung von Software. Es sind die Verantwortlichkeiten festzulegen (siehe M 2.569 Definition von Rollen und Verantwortlichkeiten bei der Software-Entwicklung) und ein Vorgehensmodell auszuwählen (siehe M 2.570 Auswahl eines Vorgehensmodells zur Software-Entwicklung). Bei der gesamten Software-Entwicklung sind gesetzliche und regulatorische Vorgaben zu berücksichtigen (siehe M 2.571 Berücksichtigung von Compliance-Anforderungen für die Software-Entwicklung).
- **Beschaffung**
  Es muss eine geeignete Entwicklungsumgebung ausgewählt werden (siehe M 4.493 Auswahl einer Entwicklungsumgebung für die Software-Entwicklung und M 2.567 Auswahl vertrauenswürdiger Entwicklungswerkzeuge). Werkzeuge für die Software-Entwicklung sollten nach standardisierten, dokumentierten Vorgehensweisen beschafft werden (siehe M 2.572 Beschaffung von Werkzeugen zur Software-Entwicklung).
- **Umsetzung**
  Während der Software-Entwicklung muss die Entwicklungsumgebung sicher eingesetzt werden (siehe M 4.494 Sicherer Einsatz einer Entwicklungsumgebung). Das Design der Software muss möglichst sicher sein (siehe M 4.495 Sicheres Systemdesign bei der Software-Entwicklung) und ebenfalls möglichst sicher implementiert werden (siehe M 2.573 Einhaltung einer sicheren Vorgehensweise bei der Software-Entwicklung und M 4.42 Implementierung von Sicherheitsfunktionalitäten in der IT-Anwendung). Die Ergebnisse der Software-Entwicklung müssen vor der produktiven Inbetriebnahme ausreichend getestet werden (siehe M 2.568 Testverfahren für Software). Der gesamte Entwicklungsprozess muss vollständig dokumentiert werden (siehe M 2.574 Ausführliche Dokumenta-

33 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Download/Vorabversionen/Baustein_Softwareentwicklung.pdf?__blob=publicationFile&v=2

tion der Software-Entwicklung) und die beteiligten Mitarbeiter sind entsprechend zu schulen (siehe M 3.97 Schulung des Projektteams für die Software-Entwicklung).

- **Betrieb**
  Zur Inbetriebnahme muss die Software sicher installiert werden (siehe M 4.496 Sichere Installation der entwickelten Software). Relevante Patches und Updates müssen umgehend angewendet werden (siehe M 2.273 Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates). Änderungen an der Konfiguration müssen sorgfältig durchgeführt werden (siehe M 4.78 Sorgfältige Durchführung von Konfigurationsänderungen). Die Integrität der Software ist regelmäßig zu überprüfen (siehe M 4.93 Regelmäßige Integritätsprüfung).
- **Aussonderung**
  Individuell entwickelte Software ist bei der Aussonderung analog zu Standardsoftware (siehe B 1.10 Standardsoftware und B 5.25 Allgemeine Anwendungen) zu behandeln.
- **Notfallvorsorge**
  Um eventuellen Ausfällen vorzubeugen sind Maßnahmen zur Notfallvorsorge zu treffen (siehe M 6.164 Notfallvorsorge bei der Software-Entwicklung). Damit sich die Software-Entwicklung bei unerwarteten Datenverlusten auf den Entwicklungssystemen nicht verzögert, sind die Entwicklungsdaten regelmäßig zu sichern (siehe M 6.32 Regelmäßige Datensicherung).

2.3.6 Zusammenfassung „Software Security“

Dieser Abschnitt hat verschiedene Verfahren, Prinzipen und Best Practices vorgestellt und somit Möglichkeiten für die Berücksichtigung von Sicherheit in der Softwareentwicklung aufgezeigt. Die Anwendung der einzelnen Vorschläge unterliegt in enera den einzelnen Entwicklungsvorhaben und Anwendungsfällen, so dass hier keine allgemeine tabellarische Kategorisierung pro Arbeitspaket (AP), wie in den Abschnitten 2.1 und 2.2, erfolgen kann. Im Folgenden wird kurz beschrieben, wenn in APs Verfahren zu Software Security eingesetzt werden, welche dieses sind:

- Als Vorgehensmodell wird im AP 2 das agile Vorgehen „SCRUM“ verwendet. In jeder der monatlichen Planungsrunde werden die Sicherheitsanforderungen erhoben und eingeplant, so dass regelmäßig „Security-by-Design“ gelebt wird.

Falls Unterstützung zu den vorgestellten Verfahren für die einzelnen APs notwendig ist, erfolgt dies in AS 12.2.4 „Governance, Compliance und Datenschutz: Erhebungen, Strukturen und Management“.

2.4 Zertifizierungen

In diesem Abschnitt werden Zertifizierung in Bezug auf Informationssicherheit, die für das Projekt enera relevant sind, kurz beschrieben. Abschnitt 2.4.1 befasst sich mit der Zertifizierung eines ISMS nach der internationalen Norm DIN ISO/IEC 27001. Abschnitt 2.4.2 erläutert die Zertifizierung von ISO 27001 nach IT-Grundschutz. In 2.4.3 werden Zertifizierungen im Rahmen des IT-Sicherheitskatalogs erörtert. Abschnitt 2.4.4 beschreibt die Zertifizierung des Smart Meter Gateway Administrators nach BSI TR 03109-6 und Abschnitt 2.4.6 erläutert die Zertifizierung eine Certification Authority (CA) für eine Public-Key-Infrastruktur, um das Sicherheitsniveau aller Teilnehmer nachzuweisen.

2.4.1 DIN ISO/IEC 27001

Die Auditierung und Zertifizierung zum Standard DIN ISO/IEC 27001 bezieht sich auf ein Informationssicherheitsmanagementsystem (Information Security Management System - ISMS), welches prozessorientiert alle für einen ausgewiesenen Geltungsbereich relevanten Werte zur Informationssicherheit umfasst. Das ISMS und die Zertifizierung dienen zum Schutz der Unternehmenswerte und Geschäftsprozesse, zum Management von Informationssicherheits-Risiken und zum Sicherheitsnachweis der Organisation gegenüber dem Gesetzgeber, Kunden, Partnern, Versicherungen und Lieferanten.

2.4.1.1 Relevanz

Die Norm mit zugehöriger Zertifizierung hat international einen großen Stellenwert. Viele Konzerne fordern von Zulieferern und Partnern ein Zertifikat zum Nachweis des Sicherheitsniveaus. Die Zertifizierung des ISMS nach DIN ISO/IEC 27001 ist unverzichtbar zur Erfüllung der Anforderungen des IT-Sicherheitskataloges und – alternativ zu ISO 27001 auf Basis IT-Grundschutz – zwingend erforderlich für die Konformität zur TR 03109-6 und zur TR 03145.

2.4.1.2 Auditierungs- und Zertifizierungsschema

Die Auditierung erfolgt in 2 Stufen („stage 1“ und „stage 2“). Wichtige Elemente die geprüft werden sind u.a. Verantwortlichkeiten, Prozesse, Dokumentationen, die Risikoanalyse, das statement of applicability, interne Audits und Managementberichte. Ebenso ist der Anhang A normativ. D.h. die dort vorgegebenen Maßnahmenziele und Maßnahmen sind grundsätzlich umzusetzen, wobei allerdings plausible Ausschlüsse erlaubt sind und bei der Umsetzung relativ große Freiheiten bestehen. DIN ISO/IEC 27002 ist nicht Gegenstand der Zertifizierung, sie bietet Unterstützung, indem sie die Controls der 27001 detaillierter beschreibt, sie ist aber nicht zwingend. Ein Zertifikat gilt (ebenso wie das für ISO 27001 auf Basis IT-Grundschutz) drei Jahre und muss jährlich durch ein Überwachungsaudit bestätigt werden.

2.4.1.3 Zertifizierungsstelle und Auditoren

Die Zertifizierung erfolgt durch eine akkreditierte Zertifizierungsstelle. Bei der Deutschen Akkreditierungsstelle (DAkkS) sind derzeit mehr als 25 Zertifizierungsstellen gelistet[34], das BSI gehört nicht dazu.
Die Auditoren werden von den Zertifizierungsstellen berufen. Sie müssen eine entsprechende Ausbildung und Erfahrung nachweisen.

2.4.2 ISO 27001 auf Basis IT-Grundschutz

ISO 27001-Zertifizierungen auf der Basis von IT-Grundschutz sind seit 2006 durch das BSI möglich. Sie integrieren die Norm DIN ISO/IEC 27001 mit der Grundschutzvorgehensweise und den Grundschutzkatalogen. Daneben gibt es noch die beiden Vorstufen „Auditor-Testat IT-Grundschutz Einstiegsstufe" und „Auditor-Testat IT-Grundschutz Aufbaustufe". Diese stellen einfachere Varianten mit geringeren Anforderungen dar und können im Regelfall durch einen zertifizierten Auditor selbständig, ohne Zertifizierungsstelle erbracht werden.

[34] Siehe auch http://www.dakks.de/content/akkreditierte-stellen-dakks.

2.4.2.1 Relevanz

Der IT-Grundschutz hat in Deutschland und teilweise der DACH-Region einen sehr hohen Stellenwert. Hinsichtlich der zugehörigen Zertifizierung sind viele Organisationen allerdings zurückhaltender, wenngleich in den letzten Jahren eine deutliche Steigerung spürbar war. Die Zertifizierung des ISMS nach ISO 27001 auf Basis IT-Grundschutz – oder alternativ DIN ISO/IEC 27002 – ist zwingend erforderlich für die Konformität zur TR 03109-6 und zur TR 03145.

2.4.2.2 Auditierungs- und Zertifizierungsschema

Vom BSI werden ein Auditierungsschema („Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz Auditierungsschema, Version 1.0“) und ein Zertifizierungsschema („Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz Zertifizierungsschema, Version 1.2“) vorgegeben, in welchen die Abläufe genau und verbindlich festgelegt sind.[35]
Eine Zusammenfassung des Auditierungs- und Zertifizierungsprozesses ist in Abbildung 8 dargestellt (Quelle: BSI).

[35] Siehe auch https://www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/Managementsystemzertifizierung/Zertifizierung27001/Zertifizierungsschema/schema_node.html;jsessionid=B8D8408880C1DFFB0872A297263557B9.1_cid341

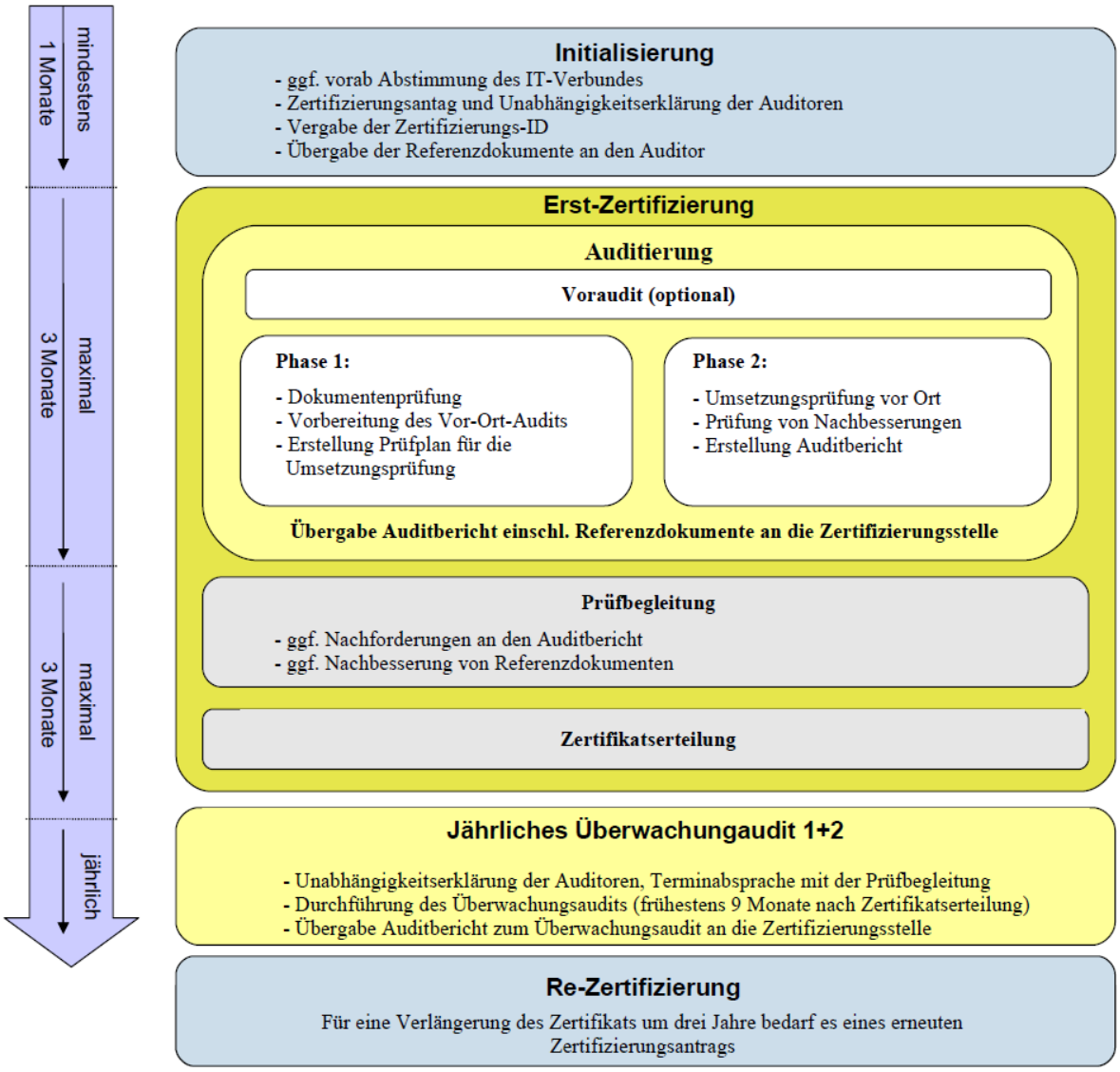


Abbildung 8: Übersicht Auditierung und Zertifizierung ISO 27001 auf Basis IT-Grundschutz (Quelle: BSI)

2.4.2.3 Zertifizierungsstelle und Auditoren

Zertifizierungsstelle ist das BSI. Zertifizierungsanträge und Unabhängigkeitserklärungen müssen beim BSI eingereicht werden. Mit der Vergabe der Zertifizierungsnummer beginnt das Audit. Der vom Auditor erstellte Auditbericht wird vom BSI genau geprüft, bevor dieses, ggf. nach der Erfüllung von Nachforderungen, das Zertifikat vergibt.
Die Auditoren müssen relevante Erfahrungen und Kenntnisse nachweisen und eine Schulung mit Prüfung beim BSI absolvieren. Sie bekommen dann für drei Jahre eine Personenzertifizierung (ebenfalls durch das BSI), welche nach Ablauf durch Nachweis ausreichender Auditaktivitäten verlängert werden kann. Die Auditoren schließen mit dem BSI einen Vertrag, stehen aber in keinem Arbeitsverhältnis zum BSI.

2.4.3 IT-Sicherheitskatalog

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

netzagentur (BNetzA) auf Grundlage von § 11 Abs. 1a des Energiewirtschaftsgesetzes (EnWG) veröffentlicht. Netzbetreiber werden verpflichtet, ihr Informationssicherheits-Managementsystem (ISMS) gemäß DIN ISO/IEC 27001 zertifizieren zu lassen, wobei neben DIN ISO/IEC 27002 zusätzlich Maßnahmen zur DIN ISO/IEC TR 27019 umzusetzen sind (Erweiterung der DIN ISO/IEC 27002 um spezifische Aspekte im Bereich der Prozesssteuerung der Energieversorgung).

2.4.3.1 Relevanz

Die Verantwortung für die Umsetzung der Vorgaben des IT-Sicherheitskatalogs haben die bei der BNetzA gelisteten Betreibern eines Strom- oder Gasnetzes. Dies gilt unabhängig davon, ob ein Netzbetreiber ein Strom- oder Gasnetz als Eigentümer oder im Rahmen eines Pachtmodells betreibt. Ausnahmen von der Umsetzungspflicht, etwa in Abhängigkeit von der Größe eines Netzbetreibers, bestehen nicht.
Die erfolgreiche Umsetzung der Anforderungen muss spätestens zum 31. Januar 2018 mit einer Zertifizierung nachgewiesen werden. Diese muss in Form einer Kopie des Zertifikats der Bundesnetzagentur vorliegen.

2.4.3.2 Auditierungs- und Zertifizierungsschema

Die Abläufe für Auditierung und Zertifizierung entsprechen im Wesentlichen denen einer reinen ISO 27001 Zertifizierung. Besonderes Augenmerk wird auf die Abgrenzung des Geltungsbereichs gelegt. Dieser muss zumindest alle TK- und EDV-Systeme des Netzbetreibers umfassen, welche direkt Teil der Netzsteuerung sind, d. h. unmittelbar Einfluss nehmen auf die Netzfahrweise. Daneben sind auch TK- und EDV-Systeme im Netz betroffen, die selbst zwar nicht direkt Teil der Netzsteuerung sind, deren Ausfall jedoch die Sicherheit des Netzbetriebs gefährden könnte.
Insbesondere zur Prüfung der Abgrenzung des Geltungsbereichs und der Risikoanalyse muss das Audit-Team einen Fachexperten hinzuziehen. Der Fachexperte soll das Auditteam bei der Einschätzung, ob alle für den Netzbetrieb notwendigen Systeme, Komponenten und Anwendungen im Scope erfasst sind und die Risikoeinschätzung korrekt durchgeführt worden ist, beraten. Er muss neben einem ingenieur- oder naturwissenschaftlichen (Fach-)Hochschulstudium mindestens drei Jahre einschlägige Berufserfahrung in der leitungsgebundenen Energieversorgung nachweisen. Die Unterstützung durch einen Fachexperten kann entfallen, sofern ein Mitglied des Audit-Teams bereits mindestens fünf Mal zusammen mit einem Fachexperten auditiert hat.

2.4.3.3 Zertifizierungsstelle und Auditoren

Die akkreditierten Stellen zur Zertifizierung des IT-Sicherheitskatalogs sind marktbekannte Stellen zur Zertifizierung von Managementsystemen. Sie können auf der Internetseite der DAkkS abgerufen werden. Stand 20170612 sind datenschutz cert GmbH, TÜV NORD CERT GmbH, TÜV Rheinland Cert GmbH, TÜV SÜD Management Service GmbH Zertifizierungsstelle und Kiwa International Cert GmbH gelistet.
Auditoren, die Netzbetreiber auditieren möchten, müssen die Anforderungen des Konformitätsbewertungsprogramms zur Akkreditierung von Zertifizierungsstellen für den IT-

Sicherheitskatalog gemäß § 11 Absatz 1a Energiewirtschaftsgesetz auf der Grundlage der ISO/IEC 27006 erfüllen. Sie müssen bei einer akkreditierten Zertifizierungsstelle lizenziert sein und eine von der Bundesnetzagentur anerkannte Schulung zu den Grundlagen der leitungsgebundenen Energieversorgung mit Strom und Gas erfolgreich absolviert haben.

2.4.4 Smart Meter Gateway Administrator

Der SMGW Admin-Betrieb ist ein Bereich mit kritischen Anwendungen. Die Umsetzung der in Kapitel 4 der TR 03109-6 aufgeführten Mindestvorgaben bzgl. der zu betrachtenden Bedrohungen und der diesen entgegenwirkenden geeigneten und angemessenen Maßnahmen sind daher im Rahmen einer Auditierung zu prüfen und durch eine abschließende Zertifizierung des ISMS zu bestätigen.

2.4.4.1 Relevanz

Die Zertifizierung ist für den SMGW Admin-Betrieb zwingend erforderlich.

2.4.4.2 Auditierungs- und Zertifizierungsschema

Die Auditierung erfolgt in den zwei Phasen Dokumentenprüfung und Prüfung der Umsetzung der in der Dokumentation beschriebenen Prozesse und Maßnahmen.
Die für die Phase der Dokumentenprüfung vorzulegende Dokumentation besteht aus der individuellen Sicherheitskonzeption des zu prüfenden SMGW Admin und beinhaltet insbesondere die unter Kapitel 4.5.1 der TR 03109-6 geforderten Dokumentation der internen Prozessabläufe sowie IT-Sicherheitsrichtlinien, die Risikoanalyse und die Ergebnisse der IT-Penetrationstests. Weitergehende Dokumente kann der Auditor nach seinem Ermessen nachfordern.
Die vorgelegte Dokumentation ist vom Auditor dahingehend zu prüfen, ob sie die geforderten Inhalte nachvollziehbar und konsistent darstellt. Festgestellte Mängel sind vor der Prüfung der Umsetzung zu beheben und erneut durch den Auditor zu prüfen.
Im Rahmen der zweiten Audit-Phase muss der Auditor zwingend die Umsetzung der geforderten Sicherheitskonzeption prüfen.
Der Auditor hat dabei insbesondere zu prüfen, ob bei der Durchführung der Risikoanalyse die in dieser Technischen Richtlinie festgelegten Assets, Schutzziele und Bedrohungen beachtet und ausreichend behandelt bzw. bewertet wurden. Ebenso ist während des Audits zu verifizieren, ob die normativen Vorgaben zu den Maßnahmen beachtet und angemessen umgesetzt wurden.

2.4.4.3 Zertifizierungsstelle und Auditoren

Eine Zertifizierung/Konformitätsprüfung nach der TR 03109-6 erfolgt immer im Zusammenhang mit einer Zertifizierung nach ISO/IEC 27001 oder ISO 27001 auf Basis von IT-Grundschutz. Somit ist entweder zwingend das BSI oder eine bei der Deutschen Akkreditierungsstelle (DAkkS) gemäß ISO/IEC 27006 für ISMS akkreditierte Organisation als Zertifizierungsstelle involviert.
Auditoren müssen sich beim BSI qualifizieren. Es gelten die „Verfahrensbeschreibung zur Kompetenzfeststellung und Zertifizierung von Personen“ und das dazugehörige Dokument

„Anforderungen an Antragsteller zur Zertifizierung als Auditor“ Diese sind in der jeweils aktuellen Version auf der Internetseite des BSI verfügbar.

2.4.5 Externer Marktteilnehmer (EMT) gemäß TR 03109

Die TR 03109-4 beschreibt eine PKI-Architektur, welche eine sichere Kommunikation mit SMGWs ermöglicht. Laut der Version 1.2 vom 09.08.2017 gehören zu den externen Marktteilnehmern „im Kontext der PKI alle Marktteilnehmer, die potentielle Kommunikationspartner eines Smart Meter Gateway im WAN sind, etwa Verteilnetzbetreiber, Messstellenbetreiber oder Lieferanten.“ Abgesehen vom SMGW Administrator, welchem eine Sonderrolle zukommt, ist also jeder Marktteilnehmer ein EMT, wenn er mit einem bzw. über ein SMGW kommuniziert.
In der Certificate Policy der Smart Metering PKI wird in der Version 1.1 vom 09.08.2017 zudem zwischen passiven und aktiven EMTs differenziert: „Ein EMT, welcher ein SMGW nutzt, um über dieses nachgelagerte Geräte (Controllable Local Systems, CLS) anzusprechen, wird als *aktiver EMT* bezeichnet. […] Ein EMT, welcher keine nachgelagerten Geräte (CLSs) anspricht bzw. steuert, sondern nur Daten empfängt, um auf Basis dieser Informationen die eigenen Geschäftsprozesse fortzuführen, wird als *passiver EMT* bezeichnet.“

2.4.5.1 Relevanz

Für eine Kommunikation mit einem bzw. über ein SMGW ist die Teilnahme an der Smart Metering PKI zwingend notwendig. Um dies zu erreichen genügt es für einen passiven EMT ein Sicherheitskonzept zu erstellen, in welchem die Anforderungen aus der SM-PKI Policy berücksichtigt werden. Ein aktiver EMT muss hingegen „eine Zertifizierung gemäß ISO/IEC 27001 nachweisen bzw. nachweisen, dass ein nach ISO/IEC 27001 zertifizierter Dritter die Leistung für ihn erbringt.“

2.4.5.2 Auditierungs- und Zertifizierungsschema

Aus der Certificate Policy: „Bei einem aktiven EMT MUSS eine entsprechende Zertifizierung alle für die PKI relevanten Geschäftsprozesse und IT-Systeme (insbesondere hinsichtlich Beantragung, Empfang und Nutzung von Schlüsseln und Zertifikaten) umfassen.
Allgemein MUSS die Zertifizierung nach ISO/IEC 27001 die Überprüfung beinhalten, dass alle Anforderungen aus TR-03109-4 und aus dieser SM-PKI Policy eingehalten werden. Das Ergebnis MUSS im Auditbericht dokumentiert werden, damit es bei Bedarf vorgelegt werden kann.“

2.4.5.3 Zertifizierungsstelle und Auditoren

Die Zertifizierung eines aktiven EMT erfolgt mit einer Zertifizierung nach ISO/IEC 27001 oder ISO 27001 auf Basis von IT-Grundschutz. Somit ist entweder zwingend das BSI oder eine bei der Deutschen Akkreditierungsstelle (DAkkS) gemäß ISO/IEC 27006 für ISMS akkreditierte Organisation als Zertifizierungsstelle involviert.
Auditoren müssen sich beim BSI qualifizieren. Es gelten die „Verfahrensbeschreibung zur Kompetenzfeststellung und Zertifizierung von Personen“ und das dazugehörige Dokument „Anforderungen an Antragsteller zur Zertifizierung als Auditor“ Diese sind in der jeweils aktuellen Version auf der Internetseite des BSI verfügbar.

2.4.6 Secure CA Operations

Nur eine sichere Certification Authority (CA) kann als Wurzel für eine Public Key Infrastruktur dienen, welche für die Sicherung von Vertraulichkeit Authentizität und Integrität von Informationen genutzt wird. Die BSI TR-03145 hat zum Ziel, CA zu unterstützen um ein angemessenes Sicherheitsniveau zu erreichen, indem organisatorische und technische Maßnahmen implementiert und Regeln für alle PKI-Teilnehmer aufgestellt werden. Die Zertifizierung dient dem Nachweis des Sicherheitsniveaus um auch das notwendige Vertrauen der anderen PKI-Teilnehmer zu erhalten.

2.4.6.1 Relevanz

Trust Center, die sich in der Smart Metering Public Key Infrastruktur (SM-PKI) als Smart Meter Certification Authority (CA) beteiligen möchten, müssen gemäß der Certificate Policy der Smart Metering-PKI eine Zertifizierung gemäß BSI TR-03145 „Secure CA Operation“ zusammen mit einer Zertifizierung ihres Informationssicherheitsmanagementsystems gemäß ISO/IEC 27001 oder ISO 27001 auf Basis IT-Grundschutz nachweisen.

2.4.6.2 Auditierungs- und Zertifizierungsschema

Es gibt seitens des BSI kein explizites Zertifizierungsschema. Ein Auditor soll das vom BSI herausgegebene Dokument „Secure CA operation, Part 2 Inspection specifications considering Trust Center (TC) instantiating as Certification Authority (CA) in Public-Key Infrastructure (PKI) with security level high'“ als Vorlage bzw. Checkliste nutzen. Für jede relevante der mehr als 200 Anforderungen muss mindestens ein Plausibilitätsnachweis erbracht (und für den Prüfbericht dokumentiert) werden, dass sie erfüllt ist.

2.4.6.3 Zertifizierungsstelle und Auditoren

Eine Zertifizierung/Konformitätsprüfung nach der TR 03145 erfolgt immer im Zusammenhang mit einer Zertifizierung nach ISO/IEC 27001 oder ISO 27001 auf Basis von IT-Grundschutz. Somit ist entweder zwingend das BSI oder eine bei der Deutschen Akkreditierungsstelle (DAkkS) gemäß ISO/IEC 27006 für ISMS akkreditierte Organisation als Zertifizierungsstelle involviert.
Auditoren müssen sich beim BSI qualifizieren. Es gelten die „Verfahrensbeschreibung zur Kompetenzfeststellung und Zertifizierung von Personen“ und das dazugehörige Dokument „Anforderungen an Antragsteller zur Zertifizierung als Auditor“ Diese sind in der jeweils aktuellen Version auf der Internetseite des BSI verfügbar.

2.4.7 Zusammenfassung „Zertifizierungen“

Dieser Abschnitt erläuterte verschiedene Zertifizierungen in Bezug auf Informationssicherheit. Diese Zertifizierungen sind im Rahmen des Projekts enera relevant. In der folgenden Tabelle 8 wird eine Zuordnung der beschriebenen Zertifizierungen zu den APs vorgenommen. Dabei ist jeder AP-Nummer ein Kurztitel zur besseren Verständlichkeit angehängt. Diese Zuordnung zu den APs erfolgte im Rahmen von AS 12.2.1 und soll durch die Schnittstellenverantwortlichen für Informationssicherheit in den APs überprüft werden. Ein „x“ pro Zelle bedeutet dabei, dass das entsprechende Gesetz eine Relevanz für das AP aufweist.

Ein „(x)“ pro Zelle heißt, dass das entsprechende Gesetz eine Relevanz für das AP ausweisen kann bzw. es gibt eine indirekte Relevanz des Gesetzes für das AP.

AP-Nummer – Kurztitel	**DIN ISO/IEC 27001**	**ISO 27001 auf Basis IT-Grundschutz**	**IT-Sicherheitskatalog**	**Smart Meter Gateway Administrator**	**Secure CA Operations**
AP1 – Digitale Konnektivität	x	x	x	x	x
AP2 – SDSP	x		(x)	(x)	
AP3 – SG-Operator	x	x	x	x	
AP4 – Rollout Netzbetriebsmittel	x	x	x		
AP5 – Flexibilisierung	x	x	x		
AP6 – Technische Entwicklung regionaler Produkte	x	x	x		
AP7 – Marktintegration regionaler Produkte	x	x			
AP8 – Energierecht	x	x			
AP9 – Neue Geschäftsmodelle	x	x			
AP10 – enera Qualifizierungscenter	x	x			
AP11 – Bürgerbeteiligung	x	x			
AP12 – Architektur und Security	x	x	x	x	x
AP13 – Nationaler/Internat. Transfer	x				
AP14 – Projektmanagement					

Tabelle 8: Relevanz der Zertifizierungen für die einzelnen APs aus enera

3 Zusammenfassung

In diesem Dokument wurden Regularien für das Thema Informationssicherheit in dem Kontext der Domäne Energie beschrieben und deren Relevanz im Projekt enera auf Basis der einzelnen Arbeitspakete beleuchtet.

In Abschnitt 2.1 wurden dafür sowohl nationale als auch internationale Gesetze, Verordnungen und gesetzliche Richtlinien erläutert. Abschließend befindet sich in Tabelle 1 ein Übersicht und Kurzzusammenfassung der genannten Gesetzestexte. In Tabelle 2 wurde die Relevanz der Gesetze für die einzelnen APs als Vorschlag erarbeitet und soll im nächsten Schritt mit den einzelnen Schnittstellenverantwortlichen für das Thema Sicherheit aus den einzelnen APs abgestimmt werden.

In Abschnitt 2.2 wurden Normen, Standards und Richtlinien aus dem Feld Informationssicherheit für die Energiedomäne beschrieben. Es handelt sich dabei um nationale und internationale Normen. Tabelle 6 gibt dabei einen Überblick über die Normen und in Tabelle 7 werden bei Relevanz die verschiedenen Normen den einzelnen APs zugeordnet. Diese Tabelle 7 ist ebenfalls als Vorschlag zu verstehen und soll im nächsten Schritt mit den einzelnen Schnittstellenverantwortlichen für das Thema Sicherheit aus den einzelnen APs abgestimmt werden.

Abschnitt 2.3 befasst sich mit Richtlinien zu Software Security und gibt stellt Verfahren, Prinzipen und Best Practices in diesem Themenfeld vor. Die Anwendung der einzelnen Methoden in den APs sollte Anwendungsfallbasiert erfolgen.
In Abschnitt 2.4 werden im Projektkontext relevante Zertifizierungen erörtert. Tabelle 8 bietet dabei eine Übersicht, welche Zertifizierungen für welches AP relevant sind. Dieser Vorschlag bzgl. der Zuordnung einzelner Zertifizierungen zu den APs soll im nächsten Schritt mit den einzelnen Schnittstellenverantwortlichen für das Thema Sicherheit aus den einzelnen APs abgestimmt werden.

Insgesamt wird aus AS 12.2.1 empfohlen, die einzelnen Regularien je nach Relevanz in der Entwicklung zu berücksichtigen. Einzelne Gesetze und Verordnungen aus Abschnitt 2.1 **müssen** dabei berücksichtigt werden. Dies gilt z.B. für kritische Infrastrukturen beim IT-Sicherheitsgesetz (siehe Abschnitt 2.1.1). Weiterhin **müssen/sollten** einzelne Normen, Standards und Richtlinien aus Abschnitt 2.2 berücksichtigt werden. Dies gilt z.B. für Strom- und Gasnetzbetreiber, die nach IT-Sicherheitskatalog ein ISMS nach ISO/IEC 27000 einführen und betreiben müssen. Die Richtlinien zu Software Security aus Abschnitt 2.3 **sollten** bei entsprechender Relevanz berücksichtigt werden.

Da sich aktuell einige Änderungen, wie auch im Text beschrieben, im Rahmen von Regularien für Informationssicherheit abzeichnen, müssen die Inhalte dieses Arbeitsschritts weitergeführt werden. Die Überwachung und Überarbeitung dieses Arbeitsschrittes 12.2.1, der Ende Juni 2017 endet, wird im Rahmen von AS 12.2.4 „Governance, Compliance und Datenschutz: Erhebungen, Strukturen und Management“ erfolgen, der bis zum Ende der Projektlaufzeit weiterläuft.

4 Abbildungsverzeichnis

Abbildung 1: PDCA-Zyklus (Quelle: BSI-Standard 100-1) 21
Abbildung 2: Erstellung eines IT-Sicherheitskonzepts mit der Standard-Absicherung (BSI-Standard 100-2) 24
Abbildung 3: Einordnung der Risikoanalyse in den Sicherheitsprozess (Quelle: BSI-Standard 200-3) 25
Abbildung 4: Darstellung der Korrelationen zwischen dem IEC 62351 und den verschiedenen Profilen (Quelle: Steffen Fries, Siemens) 28
Abbildung 5: Übersicht Normenreihe IEC 62443 (Quelle: www.dke.de) 29
Abbildung 6: Schema des V-Modells (Quelle: Michael Pätzold, S. Seyfert) 39
Abbildung 7: Schema des Wasserfallmodells nach Boehm (Quelle: http://winfwiki.wi-fom.de/index.php/Erstellung_einer_Entscheidungsgrundlage_für_die_Einführung_einer_agilen_Softwareentwicklungsmethode#Aktuelles_Vorgehensmodell) 40
Abbildung 8: Übersicht Auditierung und Zertifizierung ISO 27001 auf Basis IT-Grundschutz (Quelle: BSI) 50

5 Tabellenverzeichnis

Tabelle 1: Übersicht „Gesetze und Verordnungen“ 14
Tabelle 2: Relevanz der Gesetze für die einzelnen APs in enera 15
Tabelle 3: Anforderungen des Plan-Do-Check-Act Zyklus 17
Tabelle 4: Abschnitte und Hauptkategorien des ISO/IEC 27002 19
Tabelle 5: Ergänzende Maßnahmen der ISO/IEC 27019 in Bezug auf die ISO/IEC 27002 20
Tabelle 6: Übersichtstabelle Normen, Standards und Richtlinien 37
Tabelle 7: Relevanz der Normen, Standards und Richtlinien für die einzelnen APs aus enera 38
Tabelle 8: Relevanz der Zertifizierungen für die einzelnen APs aus enera 55

Ergebnisdokument AS 12.2.4

„Governance, Compliance und Datenschutz: Erhebungen, Strukturen und Management“

Autoren:

Alexandra Quirin, Konrad Rosmus, Ulrike Henschel (IABG), Christine Rosinger (OFFIS)

02.12.2020

Gefördert durch:

aufgrund eines Beschlusses
des Deutschen Bundestages

Historie des Dokuments:
Ergebnisdokument AS 12.2.4 in Fortschreibung des Ergebnisdokuments AS 12.2.1

Version	AS	Datum	Name (Autor)	Änderungen	Dateiname
-	12.2.1	24.02.2017	Christine Rosinger, OFFIS	Datei erstellt, 1. Vorschlag für grobe Gliederung	2017-02-27_AS12.2.1_Gesetze, Regularien, Richtlinien, Compliance, Zertifizierun-gen.docx
-	12.2.1	15.03.2017	Christine Rosinger, OFFIS	Verantwortlichkeiten in Abschnitt 3 ergänzt	2017-03-15_AS12.2.1_Gesetze, Regularien, Richtlinien, Compliance, Zertifizierungen.docx
-	12.2.1	22.03.2017	Rolf Strenge, EWE NETZ	Ergänzung 3.1.1 – 3.1.4, Umsortierung der Abschnitte	2017-03-22_AS12.2.1_Gesetze Regularien Richtlinien Compliance Zertifizierungen_RolfStrenge.docx
-	12.2.1	26.04.2017	Christian Bruns, BTC AG	Abschnitt 2.3 eingefügt	2017-03-15_AS12.2.1_Gesetze, Regularien, Richtlinien, Compliance, Zertifizierungen – CBr.docx
-	12.2.1	02.05.2017	Konrad Rosmus, IABG	Abschnitte 2.2.1, 2.2.2, 2.2.9 – 2.2.12 eingefügt	2017-05-02_AS12.2.1_Gesetze Regularien Richtlinien Compliance Zertifizierun-gen_Konrad.docx
-	12.2.1	04.05.2017	Christine Rosinger, OFFIS	Fehlende Abschnitte und Zusammenfassungen hinzugefügt, erstes Kontrolllesen	2017-05-04_AS12.2.1_Gesetze, Regularien, Richtlinien, Compliance, Zertifizierungen.docx
-	12.2.1	17.05.2017	Christine Rosinger, OFFIS	Überarbeitungen aus Telko eingebaut	2017-05-17_AS12.2.1_Gesetze, Regularien, Richtlinien, Compliance, Zertifizierungen.docx
-	12.2.1	19.05.2017	Rolf Strenge, EWE NETZ	Ergänzung zu IT-Sicherheitsgesetz	2017-05-19_AS12.2.1_Gesetze Regularien Richtlinien Compliance Zertifizierungen.docx
-	12.2.1	24.05.2017	Christine Rosinger, OFFIS	Änderungen angenommen	2017-05-24_AS12.2.1_Gesetze, Regularien, Richtlinien, Compliance, Zertifizierungen.docx

Version	AS	Datum	Name (Autor)	Änderungen	Dateiname
-	12.2.1	08.06.2017	Christine Rosinger, OFFIS	Kleine Ergänzungen in Abschnitt 3.4	2017-06-08_AS12.2.1_Gesetze, Regularien, Richtlinien, Compliance, Zertifizierun-gen.docx
-	12.2.1	10.06.2017	Christian Bruns, BTC	Ergänzungen zu BSI-Grundschutzbausteinen in 2.3	2017-06-10_AS12.2.1_Gesetze, Regularien, Richtlinien, Compliance, Zertifizierungen.docx
-	12.2.1	12.06.2017	Christine Rosinger, OFFIS	Überarbeitungen aus Telko hinzugefügt	2017-06-12_AS12.2.1_Gesetze, Regularien, Richtlinien, Compliance, Zertifizierungen.docx
-	12.2.1	13.06.2017	Konrad Rosmus, IABG	Ergänzung Kap. 2.4 Zertifizierung; Inhaltsverzeichnis	20170613_AS12.2.1_Gesetze, Regularien, Richtlinien, Compliance, Zertifizierungen.docx
-	12.2.1	14.06.2017	Christine Rosinger, OFFIS	Ergänzungen in den Abschnitten 2.3.5, 2.4 und 3	2017-06-14_AS12.2.1_Gesetze, Regularien, Richtlinien, Compliance, Zertifizierungen.docx
-	12.2.1	20.06.2017	Christine Rosinger, OFFIS	Dokument finalisiert und an AP12 Verteiler geschickt	2017-06-20_AS12.2.1_Gesetze, Regularien, Richtlinien, Compliance, Zertifizierungen.docx
1.0	12.2.1	06.07.2017	Christine Rosinger, OFFIS	Erhaltene Kommentare eingearbeitet, finalisiert. Damit ist AS12.2.1 abgeschlossen. Weitere Bearbeitung dieses Dokuments erfolgt in AS12.2.4.	2017-07-06_AS12.2.1_Gesetze, Regularien, Richtlinien, Compliance, Zertifizierungen_V1.0.docx
1.1	12.2.4	15.05.2018	Alexandra Quirin, IABG	Fortführung des Dokumentes AS 12.2.1 als AS 12.2.4	2018-05-15_AS12.2.4_Governance, Compliance und Datenschutz_V1.1
1.11	12.2.4	07.12.2018	Christine Rosinger, OFFIS	Ergänzung NISTIR 7628, ENISA geprüft und jeweilige Abschnitte angepasst	2018-12-07_AS12.2.4_Governance, Compliance und Datenschutz_V1.11

Version	AS	Datum	Name (Autor)	Änderungen	Dateiname
-	12.2.4	2018-2020	Diverse Autoren	Einzelne Aktualisierungen	<yyyy-mm-dd> _AS12.2.4_Governance, Compliance und Datenschutz_V1.<nn>.docx
1.20	12.2.4	16.11.2020	Ulrike Henschel IABG	Inhaltliche und formale Anpassungen und Aktualisierungen	2020-11-16_AS12.2.4_Governance, Compliance und Datenschutz_V1.20.docx
1.21	12.2.4	18.11.2020	Ulrike Henschel IABG	Ergänzungen aus AP12-Workshop am 17.11.2020	2020-11-18_AS12.2.4_Governance, Compliance und Datenschutz_V1.21.docx
2.0	12.2.4	02.12.2020	Ulrike Henschel IABG	Ergänzungen und Verbesserungen von OFFIS	2020-12-01_AS12.2.4_Governance, Compliance und Datenschutz_V2.0.docx

Inhalt

Inhalt 5
Abkürzungsverzeichnis 7
Abbildungsverzeichnis 9
Tabellenverzeichnis 10
1 Einleitung 11
1.1 Ausgangslage und Problemstellung 11
1.2 Zielsetzung und Vorgehensweise 12
2 Theoretische Grundlagen 13
2.1 Informationssicherheit im Energiesektor 13
2.1.1 Informationssicherheit 13
2.1.2 Cyber-Sicherheit in Industrieanlagen und -steuerungen 13
2.1.3 Kritische Infrastrukturen 13
2.2 Governance, Compliance, Datenschutz 13
2.2.1 Governance im Sinne Corporate Governance 13
2.2.2 Compliance 13
2.2.3 Datenschutz 14
3 Beschreibung und Zuordnung der Regularien 15
3.1 Methodik 15
3.2 Gesetze und Verordnungen 15
3.2.1 IT-Sicherheitsgesetz 15
3.2.2 BSI-Gesetz 16
3.2.3 EU NIS-Richtlinie 16
3.2.4 Energiewirtschaftsgesetz (EnWG) 17
3.2.5 IT-Sicherheitskatalog der Bundesnetzagentur 17
3.2.6 Messstellenbetriebsgesetz (MsbG) 18
3.2.7 Datenschutzgesetze 18
3.2.8 EEG 19
3.2.9 KWKG 20
3.2.10 Ergebnisse und Fazit 20
3.3 Normen, Standards und Richtlinien 21
3.3.1 ISO/ IEC 27000-Reihe 21

3.3.2 BSI IT-Grundschutz 27
3.3.3 BDEW Whitepaper Aktualisierung 15.5.2018 IABG 36
3.3.4 IEC 62351 37
3.3.5 IEC 62443 39
3.3.6 NISTIR 7628 39
3.3.7 NERC CIP 40
3.3.8 ENISA: Appropriate security measures for smart grids 40
3.3.9 BSI TR-03109 41
3.3.10 BSI TR-03116-3 43
3.3.11 BSI TR-03145 43
3.3.12 Common Criteria (ISO/IEC 15408) 44
3.3.13 IEEE 1686-2007 46
3.3.14 IEEE Std C37.240-2014 47
3.3.15 Ergebnisse und Fazit 48
3.4 Informationssicherheit in der Software Entwicklung 50
3.4.1 Klassische Verfahren Softwareentwicklung 51
3.4.2 Agile Verfahren in der Softwareentwicklung 52
3.4.3 Security-by-Design Prinzipien und Security Patterns 54
3.4.4 Best Practices für Software(entwicklung) 56
3.4.5 Anforderungen an Softwareentwicklung gemäß BSI 57
3.4.6 Ergebnisse und Fazit 59
3.5 Zertifizierungen 59
3.5.1 DIN ISO/IEC 27001 60
3.5.2 ISO 27001 auf Basis IT-Grundschutz 60
3.5.3 IT-Sicherheitskatalog 63
3.5.4 Smart Meter Gateway Administrator 64
3.5.5 Secure CA Operations 65
3.5.6 Ergebnisse und Fazit 66
4 Zusammenfassung und Ausblick 67
Literaturverzeichnis 68

Abkürzungsverzeichnis

Abkürzung	Bedeutung
AP	Arbeitspaket
AS	Arbeitsschritt
ASD	Adaptive Software Development
BDEW	Bundesverband der Energie- und Wasserwirtschaft e.V.
BDSG	Bundesdatenschutzgesetz
BMWi	Bundesministerium für Wirtschaft und Energie
BNetzA	Bundesnetzagentur
BSI	Bundesamt für Sicherheit in der Informationstechnik
CA	Certification Authority
CC	Common Criteria
CEM	Common Methodology for Information Technology Security Evaluation
CIP	Critical Infrastructure Protection
CP	Certificate Policy
CPU	Central Processing Unit
DACH	Deutschland, Österreich und die Schweiz
DAkkS	Deutsche Akkreditierungsstelle
DIN	Deutsches Institut für Normung e. V.
DSAnpUG-EU	Datenschutz-Anpassungs- und -Umsetzungsgesetz EU
EAL	Evaluation Assurance Level
EDV	Elektronische Datenverarbeitung
EEG	Erneuerbare-Energien-Gesetz
ENISA	Europäische Agentur für Netz- und Informationssicherheit
ENISA	European Network and Information Security Agency
EnWG	Energiewirtschaftsgesetz
EU	Europäische Union
EU-DSGV	EU Datenschutzgrundverordnung
EVG	Evaluationsgegenstand
FDD	Feature-Driven Development
HAN	Home Area Network
I&A	Identification and Authentication
ICS	Industrial Control Systems
IEC	International Electrotechnical Commission, deutsch: Internationale Elektrotechnische Kommission
IoT	Internet-of-Things
ISB	Informationssicherheitsbeauftragter
ISMS	Informationssicherheitsmanagementsystem

Abkürzung	Bedeutung
ISO	International Organization for Standardization, deutsch: Internationale Organisation für Normung
IT-SiBe	IT-Sicherheitsbeauftragter
KRITIS	Kritische Infrastrukturen
KWKG	Kraft-Wärme-Kopplungsgesetz
LMN	Local Metrological Network
MsbG	Messstellenbetriebsgesetz
NDSG	Niedersächsisches Datenschutzgesetz
NERC	North American Electric Reliability Corporation
NIS	Netz- und Informationssicherheit
NIST	National Institute of Standards and Technology
NISTIR	NIST Internal/Interagency Report
OWASP	Open Web Application Security Project
PACE	Password Authenticated Connection Establishment
PDCA	Plan-Do-Check-Act
PKI	Public Key Infrastructure
RBAC	Role Based Access Control
SIA	Seamless Integration Architecture
SINTEG	Schaufenster intelligente Energie - Digitale Agenda für die Energiewende
SMGW	Smart Meter Gateway
SM-PKI	Smart Metering - Public Key Infrastruktur
SQL	Structured Query Language
TAP	Teilarbeitspaket
TC	Trust Center
TK	Telekommunikation
TKG	Telekommunikationsgesetz
TLS	Transport Layer Security
TMG	Telemediengesetz
TR	Technische Richtlinie
TÜV	Technischer Überwachungsverein
UML	Unified Modeling Language
WAN	Wide Area Network
XP	Xtreme Programming

Abbildungsverzeichnis

Abbildung 1: PDCA-Zyklus (Quelle: BSI-Standard 100-1) 29
Abbildung 2: Vorgehensweisen nach IT-Grundschutz (BSI) 30
Abbildung 3: Erstellung eines IT-Sicherheitskonzepts mit der Standard-Absicherung (BSI-Standard 200-2) 30
Abbildung 4: Einordnung der Risikoanalyse in den Sicherheitsprozess (Quelle: BSI-Standard 200-3) 33
Abbildung 5: Darstellung der Korrelationen zwischen dem IEC 62351 und den verschiedenen Profilen (Quelle: Steffen Fries, Siemens) 38
Abbildung 6: Übersicht Normenreihe IEC 62443 (Quelle: www.dke.de) 39
Abbildung 7: Schema des V-Modells (Quelle: Michael Pätzold, S. Seyfert) 51
Abbildung 8: Schema des Wasserfallmodells 52
Abbildung 9: Übersicht Auditierung und Zertifizierung ISO 27001 auf Basis IT-Grundschutz (Quelle: BSI) 62

Tabellenverzeichnis

Tabelle 1: Übersicht „Gesetze und Verordnungen“ 20
Tabelle 2: Relevanz der Gesetze für die einzelnen APs in enera 21
Tabelle 3: Anforderungen des Plan-Do-Check-Act Zyklus 23
Tabelle 4: Abschnitte und Hauptkategorien des ISO/IEC 27002 25
Tabelle 5: Ergänzende Maßnahmen der ISO/IEC 27019 in Bezug auf die ISO/IEC 27002 27
Tabelle 6: Übersichtstabelle Normen, Standards und Richtlinien 49
Tabelle 7: Relevanz der Normen, Standards und Richtlinien für die einzelnen APs in enera 50
Tabelle 8: Relevanz der Zertifizierungen für die einzelnen APs aus enera 66

Ergebnisdokument AS 12.2.4

„Governance, Compliance und Datenschutz: Erhebungen, Strukturen und Management“

1 Einleitung

1.1 Ausgangslage und Problemstellung

Enera ist eins der fünf durch das Bundesministerium für Wirtschaft und Energie (BMWi) geförderten Projekte des Förderprogramms „Schaufenster intelligente Energie – Digitale Agenda für die Energiewende“ (SINTEG)[1]. Im Projekt werden Lösungen zu den drei Themenschwerpunkten Netz, Markt und Daten in der Modellregion im Nordwesten Niedersachsens entwickelt und erprobt. Das **Arbeitspaket (AP) 12** innerhalb dieses Projektes beschäftigt sich mit der informationstechnischen Entwicklung der enera Gesamtarchitektur inklusive eines Informationssicherheitskonzepts. Das Arbeitspakt 12 untergliedert sich in Teilarbeitspakete. Das **Teilarbeitspaket (TAP) 12.2** befasst sich mit dem Informationssicherheitskonzept.

Der dazugehörige **Arbeitsschritt (AS) 12.2.4** mit dem Titel „Governance, Compliance und Datenschutz: Erhebungen, Strukturen und Management“ ist eine Fortschreibung des AS 12.2.1 zum Thema „Gesetze, Richtlinien, Compliance und Zertifizierungen“. AS 12.2.1 befasst sich mit der Frage, welche Regularien zu beachten sind, und beschäftigt sich mit Compliance und vorgeschriebene Zertifizierungen im Bereich der Informationssicherheit und des Energiesektors. Identifizierte Regularien werden nach Relevanz den APs zugeordnet und sind von den Schnittstellenverantwortlichen für Informationssicherheit der APs zu überprüfen. Soweit möglich wurden Regularien, Compliance und Zertifizierungen nach „müssen“, „müssen / sollten“ und „sollten“ kategorisiert.

Aufgrund einer dynamischen Umwelt und technologischer Weiterentwicklungen bzw. Innovationen werden Regularien, Compliance und Zertifizierungen mit der Zeit an den „Stand der Technik“[2] angepasst. Herausforderung für den AS 12.2.4 ist es, diese Änderungen der Regularien, Compliance und Zertifizierungen über den gesamten Projektverlauf von enera zu erfassen und entsprechend in den einzelnen APs zu berücksichtigen.

[1] Siehe auch die Seite des SINTEG-Förderprogramms auf der Homepage des BMWi https://www.bmwi.de/Redaktion/DE/Artikel/Energie/sinteg.html.

[2] Der Bundesverband IT-Sicherheit e.V. (TeleTrust) hat zum Thema „Stand der Technik“ eine Handreichung mit technischen und organisatorischen Maßnahmen erstellt, die auf folgender Webseite eingesehen werden kann: https://www.teletrust.de/fileadmin/docs/fachgruppen/ag-stand-der-technik/2020-01_TeleTrusT_Handreichung_Stand_der_Technik_in_der_IT-Sicherheit_DEU.pdf.

1.2 Zielsetzung und Vorgehensweise

Ziel im AS 12.2.4 war es, die in dem Ergebnisbericht zu AS 12.2.1 identifizierten Regularien, Compliance-Empfehlungen und Zertifizierungen im Bereich Informationssicherheit bis zum Projektende 2020 zu überwachen und bei Bedarf zu aktualisieren und zu erweitern bzw. zu ergänzen. Der Fokus liegt auf den Regularien, Compliance-Empfehlungen und Zertifizierungen, die in den einzelnen APs zu berücksichtigen sind. Die Zuordnungen der Regularien, Compliance-Empfehlungen und Zertifizierungen sind unter Berücksichtigung der Aktualisierungen zu den APs zu überprüfen. Die Zuordnung in die Kategorien „müssen“, „müssen / sollten“ und „sollten“ ist zu prüfen.

Dazu werden zunächst in **Kapitel 2** die theoretischen Grundlagen zu Informationssicherheit im Energiesektor sowie Governance, Compliance und Datenschutz vorgestellt.

In **Kapitel 3** erfolgt eine Eingrenzung und Beschreibung der Vorgehensweise für das Monitoring von Veränderungen in Regularien, Compliance und Zertifizierungen. Die Beschreibungen der Regularien, Compliance und Zertifizierungen aus AS 12.2.1 werden um Aktualisierungen ergänzt, und die Zuordnung der Regularien, Compliance und Zertifizierungen zu den einzelnen APs wird auf Basis der Aktualisierungen ggf. aktualisiert dargestellt.

Das Dokument schließt mit einer Zusammenfassung und einem Ausblick in **Kapitel 4**Fehler! V erweisquelle konnte nicht gefunden werden..

2 Theoretische Grundlagen

In diesem Kapitel wird auf die Informationssicherheit im Energiesektor eingegangen, und es werden wichtige Begrifflichkeiten wie Regularien, Compliance, Zertifizierungen sowie Governance und Datenschutz definiert.

2.1 Informationssicherheit im Energiesektor

In diesem Kapitel werden die zentralen Begrifflichkeiten Informationssicherheit, Sicherheit in Industrieanlagen und kritische Infrastrukturen vorgestellt.

2.1.1 Informationssicherheit

„Informationssicherheit hat den Schutz von Informationen als Ziel. Dabei können Informationen sowohl auf Papier, in Rechnern oder auch in Köpfen gespeichert sein. IT-Sicherheit beschäftigt sich an erster Stelle mit dem Schutz elektronisch gespeicherter Informationen und deren Verarbeitung. Der Begriff "Informationssicherheit" statt IT-Sicherheit ist daher umfassender und wird zunehmend verwendet.“ [BSI 20]

2.1.2 Cyber-Sicherheit in Industrieanlagen und -steuerungen

„Industrial Control System (ICS) Security befasst sich mit der IT-Sicherheit in den Bereichen Fabrikautomation und Prozesssteuerung.“ [BSI 18]

2.1.3 Kritische Infrastrukturen

„Kritische Infrastrukturen (KRITIS) sind Organisationen oder Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden.“ [BSI 18]

2.2 Governance, Compliance, Datenschutz

In diesem Kapitel werden die Begriffe Governance, Compliance und Datenschutz aus dem Dokumententitel definiert.

2.2.1 Governance im Sinne Corporate Governance

„Unter dem Begriff der Corporate Governance fasst man sämtliche Prozesse der Leitung und Überwachung eines Unternehmens zusammen. Dies betrifft die interne Ordnung inklusive Regelungen und Richtlinien, Überwachungsfunktionen und deren Mittel. Ursprünglich beschrieb der Begriff lediglich Verfahren der Kontrolle der Anteilseigner gegenüber dem Management eines Unternehmens. Mittlerweile hat man ihn jedoch ausgeweitet, so dass z.B. auch Beziehungen zwischen verschiedenen Stakeholdern, Binnenstrukturen der Unternehmensführung oder externe Faktoren stärker Berücksichtigung finden.“ [CONT 18]

2.2.2 Compliance

„Engl. Begriff, sinngemäß Einhaltung von Gesetzen, Regeln und Normen. Ursprüngl. auf die Bankwirtschaft und das Gesundheitsmanagement begrenzt, inzw. breit eingesetzt, z.B. IT-

Compliance, Global Compliance, Tax Compliance, Customs Compliance, Datenschutz Compliance, das mithilfe von Compliance Management Systemen (CMS) und personifiziert durch den Compliance Officer durchgeführt wird (u.a. im Rahmen des Risikomanagements).“ [GABL 20]

2.2.3 Datenschutz

„Datenschutz soll den Einzelnen davor schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird. Mit Datenschutz wird daher der Schutz personenbezogener Daten vor etwaigem Missbrauch durch Dritte bezeichnet (nicht zu verwechseln mit Datensicherheit). Für den Begriff "Datenschutz" existieren zwei englische Übersetzungen: Dabei bezeichnet "data protection" den Datenschutz als Rechtsbegriff. "Privacy" zielt dagegen auf die gesellschaftliche Lebensweise ab (Schutz der Privatsphäre) und wird überwiegend im amerikanischen Sprachumfeld und mittlerweile auch im EU-Raum vermehrt genutzt.“ [BSI 18]

3 Beschreibung und Zuordnung der Regularien

Zunächst erfolgt in diesem Kapitel die Vorstellung der Methodik für das Monitoring und Ergänzen von Regularien, die in AS 12.2.1 nicht aufgeführt sind. Anschließend werden die bereits in AS 12.2.1 erfassten Regularien sowie Hinweise zu Compliance und Zertifizierungen durch die erforderlichen Aktualisierungen ergänzt und ihre Zuordnungen zu den APs unter Berücksichtigung der Aktualisierungen überprüft.

3.1 Methodik

Der AS 12.2.4 ist eine Fortführung des AS 12.2.1. Die Gliederung und Auflistung der Gesetze, Richtlinien, Compliance und Zertifizierungen des AS 12.2.1 wird in AS 12.2.4 beibehalten:

- Gesetze und Verordnungen
- Normen, Standards und Richtlinien
- Informationssicherheit in der Softwareentwicklung
- Zertifizierungen

Ergänzende Regularien werden in die bestehende Gliederung aufgenommen. Auch sie sind ab Initialisierung des Arbeitsschrittes AS 12.2.4 zu monitoren, und die Aktualisierungen sind im Ergebnisdokument AS 12.2.4 zu dokumentieren und ggf. fortzuschreiben. Regularien, die im AS 12.2.1 nicht aufgeführt werden, jedoch im Hinblick auf die Informationssicherheit im Energiesektor wesentlich sind, sind im Ergebnisdokument AS 12.2.4 zu ergänzen.

3.2 Gesetze und Verordnungen

Dieser Abschnitt gibt eine Kurzbeschreibung verschiedener im Kontext von Informationssicherheit relevanter Gesetze, Verordnungen und gesetzlicher Richtlinien. Dabei werden sowohl nationale als auch internationale Regularien beleuchtet.

3.2.1 IT-Sicherheitsgesetz[3]

Das IT-Sicherheitsgesetz (Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme) ist ein am 25.07.2015 in Kraft getretenes Gesetz zur Verbesserung des Schutzes der Informationssicherheit von besonders gefährdeten Infrastrukturen (sogenannten kritischen Infrastrukturen, KRITIS) wie Energie, Wasser, Gesundheit oder Telekommunikation.

Das Gesetz ist ein Artikelgesetz, welches Änderungen in verschiedenen anderen Gesetzen bewirkt hat, darunter das BSI-Gesetz, das Energiewirtschaftsgesetz (EnWG), das Telemediengesetz (TMG) und das Telekommunikationsgesetz (TKG).

[3] Informationen des BSI zum IT-Sicherheitsgesetz können unter https://www.bsi.bund.de/DE/Themen/Industrie_KRITIS/IT-SiG/it_sig_node.html abgerufen werden.

Um zu ermitteln, welche Unternehmen zu den kritischen Infrastrukturen zählen, für die diese Anforderungen gelten, ist die Verordnung zur Bestimmung Kritischer Infrastrukturen (BSI-Kritisverordnung - BSI-KritisV)[4] gemäß § 10 Absatz 1 des BSI[5]-Gesetzes in Kraft getreten.

Die dort definierten Schwellwerte geben den Wert vor, bei dessen Erreichen oder dessen Überschreitung der Versorgungsgrad einer Anlage oder Teilen davon als bedeutend im Sinne von § 10 Absatz 1 Satz 1 des BSI-Gesetzes anzusehen ist. Diese Schwellwerte sind in Energiemengen ausgedrückt und leiten sich jeweils aus dem Durchschnittsverbrauch von 500.000 Personen ab.

3.2.2 BSI-Gesetz[6]

Das „BSI-Gesetz“ ist das Gesetz, das die Aufgaben und Befugnisse des Bundesamts für Sicherheit in der Informationstechnik (BSI) festlegt.

Besondere Relevanz hat das BSI-Gesetz dadurch bekommen, dass durch das IT-Sicherheitsgesetz Änderungen in Bezug auf die kritischen Infrastrukturen (KRITIS) eingeflossen sind.

Die wesentlichen Änderungen diesbezüglich sind:

- Betreiber Kritischer Infrastrukturen müssen gemäß § 8a die Einhaltung von IT-Sicherheit nach dem Stand der Technik[7] gegenüber dem BSI nachweisen. Das BSI darf im Einvernehmen mit den Aufsichtsbehörden die Beseitigung von Sicherheitsmängeln anordnen.
- Das BSI ist gemäß § 8b die zentrale Meldestelle für die IT-Sicherheitsvorfälle der KRITIS Unternehmen. Diese müssen dem BSI erhebliche Störungen ihrer IT melden, sofern sie Auswirkungen auf die Verfügbarkeit kritischer Dienstleistungen haben können oder diese akut bedrohen.
- Sofern bei einem Betreiber Kritischer Infrastrukturen meldepflichtige Störungen der IT auftreten, darf das BSI auch die Hersteller der entsprechenden IT-Produkte und Systeme zur Mitwirkung verpflichten.
- Zu den Aufgaben des BSI gehört es auch, IT-Produkte auf ihre Sicherheit hin zu untersuchen.

3.2.3 EU NIS-Richtlinie[8]

Die EU NIS-Richtlinie – NIS steht dabei für Netz- und Informationssicherheit – wurde parallel zur Europäischen Cybersicherheitsstrategie von der Europäischen Kommission entworfen und im Juli 2016 verabschiedet. Diese Richtlinie soll dazu dienen, die Netz- und Informationssicherheit in Europa zu verbessern und dabei private Betreiber von Netzwerk- und Informations-

[4] Die BSI-KritisV kann unter https://www.gesetze-im-internet.de/bundesrecht/bsi-kritisv/gesamt.pdf abgerufen werden.
[5] BSI steht für Bundesamt für Sicherheit in der Informationstechnik.
[6] Der Text des BSI-Gesetzes kann unter https://www.gesetze-im-internet.de/bsig_2009/ abgerufen werden.
[7] Siehe auch Veröffentlichung „Handreichung zum „Stand der Technik““ von TeleTrust: https://www.teletrust.de/fileadmin/docs/fachgruppen/ag-stand-der-technik/2020-01_TeleTrusT_Handreichung_Stand_der_Technik_in_der_IT-Sicherheit_DEU.pdf.
[8] Die EU NIS Richtlinie kann unter http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016L1148&from=DE abgerufen werden.

systemen zu verpflichten die entsprechenden Mindestanforderungen zu gewährleisten. Zusätzlich muss ein Berichtssystem zwischen den einzelnen Mitgliedsstaaten untereinander und mit der ENISA9 (Europäische Agentur für Netz und Informationssicherheit) etabliert werden.

Bis Mai 2018 muss die Richtlinie durch gesetzliche Anpassung ins deutsche Recht übernommen werden. Die Richtlinie entspricht allerdings in vielen Punkten dem deutschen IT-Sicherheitsgesetz und es muss nur eine Mindestharmonisierung erfolgen, das heißt, es müssen nur dort Anpassungen erfolgen, wo das Mindestschutzniveau der Richtlinie unterschritten wird. Relevant ist diese Richtlinie für „Betreiber wesentlicher Dienste und Anbieter digitaler Dienste“ und sie ist somit relevant für das Projekt enera.

3.2.4 Energiewirtschaftsgesetz (EnWG)

Der § 11 des EnWG wurde ebenfalls durch das IT-Sicherheitsgesetz geändert. Hier werden Anforderungen hinsichtlich der die IT-Sicherheit an Netz- und Anlagenbetreiber gestellt, die teilweise Ausnahmen zu den Vorgaben aus dem geänderten BSI-Gesetz darstellen. Unter anderem wird den Netzbetreibern die Einhaltung des sogenannten IT-Sicherheitskatalogs der Bundesnetzagentur auferlegt.

Weiterhin wird in § 14a für steuerbare Verbrauchseinrichtungen in der Niederspannung vorgeschrieben, die Anforderungen des Messstellenbetriebsgesetzes (siehe Abschnitt 3.2.6) zu berücksichtigen.

3.2.5 IT-Sicherheitskatalog[10] der Bundesnetzagentur

Der IT-Sicherheitskatalog gemäß §11 Absatz 1a Energiewirtschaftsgesetz der Bundesnetzagentur (BNetzA) verpflichtet Strom- und Gasnetzbetreiber zur Einhaltung von konkreten Vorgaben in Bezug auf Informationssicherheit. Dazu zählen im Wesentlichen die Einführung und der Betrieb eines Informationssicherheitsmanagementsystems (ISMS) gemäß DIN ISO/IEC 27001 unter Berücksichtigung der ergänzenden Normen DIN ISO/IEC 27002 und DIN ISO/IEC 27019 gemäß einem spezifischen Zertifizierungsschema. Für bestimmte Anlagentypen können der VGB Standard S-175 „IT-Sicherheit für Erzeugungsanlagen“[11] sowie das BDEW Whitepaper (siehe Kapitel 3.3.3berücksichtigt werden.

Die zunächst bis zum 31. Januar 2018 lautende Umsetzungsfrist Frist zur Erfüllung dieser Anforderungen durch die Vorlage eines von einer akkreditierten Zertifizierungsstelle ausgestellten Zertifikats wurde verlängert und endet nun am 31. März 2021, wobei ein Ansprechpartner bereits bis zum 28. Februar 2019 zu benennen war.

Die Vorgaben an die Zertifizierungsstellen für diese Zertifizierung werden in einem eigenen Konformitätsbewertungsprogramm festgelegt (Konformitätsbewertungsprogramm zur Akkreditierung von Zertifizierungsstellen für den IT-Sicherheitskatalog gemäß § 11 Absatz 1a Energiewirtschaftsgesetz auf der Grundlage der ISO/IEC 27006).

---

[9] Siehe https://www.enisa.europa.eu/.

[10] Der Text des IT-Sicherheitskatalogs kann unter https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Energie/Unternehmen_Institutionen/Versorgungssicherheit/IT_Sicherheit/IT_Sicherheitskatalog_08-2015.pdf;jsessionid=DBAE00EEDD0E4FC2E7E1EB36C21E55AF?__blob=publicationFile&v=1 abgerufen werden.

[11] Beschreibung des Standard siehe https://www.vgb.org/shop/s-175.html

3.2.6 Messstellenbetriebsgesetz (MsbG)[12]

Das MsbG beschreibt Regelungen von Messstellen der leitungsgebundenen Energieversorgung inkl. moderner Messeinrichtungen und intelligenter Messsysteme13, sowie der Ausgestaltung des Messbetriebs. Dabei werden technische Mindestanforderungen an den Einsatz von intelligenten Messsystemen und deren Kommunikation festgelegt. Es werden auch insbesondere die Sicherheitsanforderungen durch die Schutzprofile und Technischen Richtlinien (TR) des BSI, z.B. BSI-CC-PP-0073-2014 (Schutzprofil Smart Meter Gateway), BSI-CC-PP-0077-V2-2015 (Schutzprofil Sicherheitsmodul), BSI TR-03109 (verschiedene Technische Richtlinien), festgelegt, sowie entsprechende Zertifikatsnachweise (z.B. Zertifizierung der Gateway-Administratoren) vorgeschrieben. Außerdem werden Regelungen zur Erhebung, Verarbeitung und Nutzung personenbezogener Daten beschrieben (Datenschutz). Dieses Gesetz ist am 02.09.2016 in Kraft getreten und ist für zukünftig eingebaute intelligente Messsysteme relevant. Dabei müssen Messstellenbetreiber, wenn technisch möglich (§ 30 MsbG) und wirtschaftliche vertretbar (§ 31 MsbG), Letztverbraucher mit über 6000 Kilowattstunden pro Jahr und Anlagenbetreiber mit einer installierten Leistung über 7 Kilowatt mit intelligenten Messsystemen ausstatten. Unter diesen Grenzwerten können ebenfalls intelligente Messsysteme durch den Messstellenbetreiber eingesetzt werden, es müssen aber mindestens moderne Messeinrichtungen verwendet werden (§ 29 MsbG).

3.2.7 Datenschutzgesetze

Dieses Kapitel geht auf die Datenschutzgesetze auf Landes-, Bundes- und EU-Ebene ein.

3.2.7.1 Einführung in die Datenschutzgesetze

Insgesamt gibt es Datenschutzgesetze auf verschiedenen Ebenen. In diesem Dokument werden zum einen das Niedersächsische Datenschutzgesetz (NDSG) aufgrund der Örtlichkeit der Modellregion in Abschnitt 3.2.7.2, das Bundesdatenschutzgesetz (BDSG) in Abschnitt 3.2.7.3 und die EU Datenschutzgrundverordnung (EU-DSGVO) in Abschnitt 3.2.7.4 kurz beschrieben. Bei einem Transfer in andere Modellregionen bzw. Regionen anderer Bundesländer müssen evtl. andere Landesdatenschutzgesetze berücksichtigt werden.

3.2.7.2 Niedersächsisches Datenschutzgesetz (NDSG)[14]

Das Niedersächsische Datenschutzgesetz (NDSG) gilt für die Verarbeitung personenbezogener Daten durch Behörden und sonstige öffentliche Stellen. Ob die einzelnen Unternehmen in enera zu diesen "Behörden und sonstigen öffentlichen Stellen" zu zählen, muss noch geklärt werden. Es gibt in § 2 Abs. 3 eine Ausnahme für "öffentliche Wettbewerbsunternehmen", hier sollen dann nur die §§ 19, 21 bis 23 zur „Datenschutzkontrolle“ sowie § 8 zur „Verfahrensbeschreibung“ und § 26 zum „Fernmessen und Fernwirken“ gelten, um die Chancengleichheit im

[12] Der Text des MsbG kann unter https://www.gesetze-im-internet.de/messbg/ abgerufen werden.
[13] Die Definitionen der Begriffe „moderne Messeinrichtung“ und „intelligenten Messsystems“ sind in § 2 MsbG festgelegt.
[14] Das NDSG kann unter http://www.lfd.niedersachsen.de/download/32372/Niedersaechsisches_Datenschutzgesetz_Stand_12.12.2012_.pdf abgerufen werden.

Wettbewerb zu sichern. Zu ebendiesem § 26 (Fernmessen und Fernwirken) schreibt der Datenschutzbeauftragte in seinem Kommentar[15] zum NDSG auf Seite 136, dass "für Stromlieferanten heutzutage in der Regel das BDSG Anwendung finden wird". Daher findet das NDSG in enera keine Anwendung.

3.2.7.3 Bundesdatenschutzgesetz (BDSG)[16]

Das BDSG gilt nach § 1 Abs. 2 für "die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch" (neben öffentlichen Stellen) "3. nicht-öffentliche Stellen, soweit sie die Daten unter Einsatz von Datenverarbeitungsanlagen verarbeiten, nutzen oder dafür erheben oder die Daten in oder aus nicht automatisierten Dateien verarbeiten, nutzen oder dafür erheben, ...". Damit ist das BDSG im Projekt enera zu berücksichtigen, so lange es nicht durch andere Gesetze ersetzt wird, und Prinzipien z.B. wie Datensparsamkeit und Datenvermeidung (§ 3a) sind umzusetzen.

Eine neue Fassung des BDSG gilt seit dem 25. Mai 2018; sie ist mit der Datenschutz-Grundverordnung (DSGVO) anwendbar.

3.2.7.4 EU Datenschutzgrundverordnung (EU-DSGVO)[17]

Die Datenschutz-Grundverordnung (DSGVO) ist eine Verordnung der Europäischen Union, mit der die Regeln zur Verarbeitung personenbezogener Daten vereinheitlicht werden. Sie gilt seit dem 25. Mai 2018 unmittelbar in allen EU-Mitgliedstaaten.

Darin eröffnen nur sogenannte Öffnungsklauseln den einzelnen Ländern Möglichkeiten, nationale Regelungen zu erlassen, es darf aber nicht der Datenschutz durch nationale Regelungen abgeschwächt oder verstärkt werden. In Deutschland wurde die EU-DSGVO durch das Datenschutz-Anpassungs- und -Umsetzungsgesetz EU (DSAnpUG-EU) umgesetzt und ins deutsche Recht übernommen.

3.2.8 EEG

Das EEG ist das Erneuerbare-Energien-Gesetz für den Ausbau der Erneuerbaren Energien. Dieser Ausbau soll laut § 1 „stetig, kosteneffizient und netzverträglich erfolgen“ und damit die Ziele der EU bzgl. des Anteils an erzeugtem Strom aus erneuerbaren Energien erfüllen. Auf Informationssicherheitsaspekte wird in diesem Gesetz nicht explizit eingegangen. In verschiedene Paragraphen wird auf das MsbG und somit den Stand der Technik[18] und das BSI verwiesen.

---

[15] Der Kommentar des Datenschutzbeauftragten des Landes Niedersachsens ist unter http://www.lfd.niedersachsen.de/download/32433/NDSG_mit_Kommentar_Stand_November_2014_.pdf abrufbar.

[16] Der Text des BDSG kann unter https://www.gesetze-im-internet.de/bdsg_2018/index.html abgerufen werden.

[17] Der Text der EU-DSGVO kann unter https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016R0679&from=DE abgerufen werden.

[18] Siehe auch https://www.teletrust.de/fileadmin/docs/fachgruppen/ag-stand-der-technik/2020-01_TeleTrusT_Handreichung_Stand_der_Technik_in_der_IT-Sicherheit_DEU.pdf.

3.2.9 KWKG

Das KWKG ist das Kraft-Wärme-Kopplungsgesetz und dient der Erhaltung, der Modernisierung und dem Ausbau der Kraft-Wärme-Kopplung. Auch das KWKG verweist nicht explizit auf Informationssicherheitsmaßnahmen und bezieht sich an verschiedenen Stellen auf das MsbG, so dass auch hier der Stand der Technik umgesetzt werden muss, der teilweise durch das BSI vorgegeben wird.

3.2.10 Ergebnisse und Fazit

In der folgenden Tabelle 1 sind die in diesem Abschnitt 3.2 beschriebenen Gesetze und Verordnungen überblicksartig dargestellt, wobei ihre geografische Gültigkeit eingeordnet und der entsprechende Inhalt in Bezug auf Informationssicherheit kurz erläutert wird.

Name Gesetz	Gültigkeit			Inhalt – kurz
	regional	national	international	
IT-Sicherheitsgesetz		x		Vorgaben für den Schutz von kritischen Infrastrukturen; Meldepflichten etc.
BSI-Gesetz		x		Vorgaben für Aufgaben und Befugnisse des BSI; Nachweis Stand der Technik, BSI als zentrale Meldestelle etc.
EU-NIS-Richtlinie			x	Vorgaben für Netz- und Informationssicherheit in Europa; Umsetzung und Gewährleistung von Mindestanforderungen etc.
EnWG		x		Vorgaben zu IT-Sicherheit an Netz- und Anlagenbetreiber; Anwendung des IT-Sicherheitskatalogs und MsbG etc.
IT-Sicherheitskatalog		x		Vorgaben zu Informationssicherheit für Strom- und Gasnetzbetreiber; Betrieb eines ISMS nach DIN ISO/IEC 27001/27002/27019 etc.
MsbG		x		Vorgaben zu Sicherheitsanforderungen für Messeinrichtungen der Energieversorgung; Umsetzung durch Schutzprofile und TRs des BSI etc.
NDSG	x			Datenschutzvorgaben in Niedersachsen
BDSG		x		Datenschutzvorgaben in Deutschland
EU-DSGVO			x	Datenschutzvorgaben in der Europäischen Union
EEG		x		Indirekte Vorgaben zu Informationssicherheit
KWKG		x		Indirekte Vorgaben zu Informationssicherheit

Tabelle 1: Übersicht „Gesetze und Verordnungen“

In der folgenden Tabelle 2 werden die Gesetze, die Informationssicherheitsaspekte behandeln, den einzelnen Arbeitspaketen (AP) innerhalb des enera-Projekts zugeordnet und somit deren Relevanz für die einzelnen APs aufgezeigt. Dabei ist jeder AP-Nummer ein Kurztitel zur besseren Verständlichkeit angehängt. Ein „x“ pro Zelle bedeutet dabei, dass das entspre-

chende Gesetz eine Relevanz für das AP aufweist. Ein „(x)“ pro Zelle heißt, dass das entsprechende Gesetz eine Relevanz für das AP ausweisen kann bzw. es gibt eine indirekte Relevanz des Gesetzes für das AP.

AP-Nummer – Kurztitel	IT-Sicherheitsgesetz	EU-NIS-Richtlinie	BSI-Gesetz	EnWG	IT-Sicherheitskatalog	MsbG	Datenschutzgesetze			EEG	KWKG
							NDSG	BDSG	EU-DSGVO		
AP1 – Digitale Konnektivität	x	x	x	x	x	x	x	x	x		
AP2 – SDSP	(x)	x	x				x	x	x		
AP3 – SG-Operator	x	x	x	x	x		x	x	x		
AP4 – Rollout Netzbetriebsmittel	x	x	x	x	x	(x)					
AP5 – Flexibilisierung	x	x	x	x	x	(x)	(x)	(x)	(x)		
AP6 – Technische Entwicklung regionaler Produkte	x	x	x	x	x	(x)	x	x	x		
AP7 – Marktintegration regionaler Produkte							x	x	x		
AP8 – Energierecht											
AP9 – Neue Geschäftsmodelle							x	x	x		
AP10 – enera Qualifizierungscenter							x	x	x		
AP11 – Bürgerbeteiligung						(x)	x	x	x		
AP12 – Architektur und Security	x	x	x	x	x	x	x	x	x		
AP13 – Nationaler/Internat. Transfer									x		
AP14 – Projektmanagement											

Tabelle 2: Relevanz der Gesetze für die einzelnen APs in enera

3.3 Normen, Standards und Richtlinien

Dieses Kapitel beschreibt verschiedene Normen, Standards und Richtlinien für Informationssicherheit, die für das Projekt enera relevant sind. In den Abschnitten 3.3.1 bis **Fehler! Verweisquelle konnte nicht gefunden werden.** werden die identifizierten Normen, Standards und Richtlinien kurz beschrieben. Abschnitt 3.3.15 enthält abschließend eine Übersicht und zusammenfassende Darstellung der Standards mit Angaben zur Relevanz für die einzelnen AP im Projekt.

3.3.1 ISO/ IEC 27000-Reihe

Zunächst wird ein Überblick zum Thema ISO/ IEC 27000-Reihe gegeben. Anschließend wird auf die Standards ISO 27000, 27001, 27002 und ISO/ IEC 27019 einzeln eingegangen.

3.3.1.1 Einführung zur ISO/ IEC 27000-Reihe

ISO steht für „International Organization for Standardization“ (deutsch: Internationale Organisation für Normung); diese ist eine internationale Vereinigung von Normungsorganisationen, die internationale Normen erarbeitet. Die IEC, auf Deutsch „Internationale Elektrotechnische Kommission“ ist ein internationales Normungsgremium, das Standards und Normen für den Bereich der Elektrotechnik und der Elektronik entwickelt. Sowohl die ISO als auch die IEC haben ihren Sitz in Genf in der Schweiz.
Die ISO/IEC 27000-Reihe (auch mit ISO/IEC 27000-Familie bezeichnet) ist eine Reihe von Standards zur Informationssicherheit, welche von der International Organization for Standardization (ISO[19]) und der International Electrotechnical Commission (IEC[20]) herausgegeben wird.

3.3.1.2 ISO 27000

Die internationale Norm ISO/IEC 27000 bildet den Rahmen für die ISO/IEC 27000-Familie. Sie definiert häufig verwendete Fachbegriffe und gibt einen Kurzüberblick über die einzelnen Standards.

3.3.1.3 ISO 27001

Die internationale Norm ISO/IEC 27001 (deutsche Fassung DIN ISO/IEC 27001) wurde erarbeitet, um Anforderungen für die Einrichtung, Implementierung, Wartung und laufende Verbesserung eines **Informationssicherheitsmanagementsystems (ISMS**) festzulegen.

Mit diesem sollen Vertraulichkeit, Integrität und Verfügbarkeit von Informationen durch Anwendung eines Risikomanagement-Prozesses geschützt werden, und interessierte Parteien sollen darauf vertrauen können, dass mit Risiken angemessen umgegangen wird.

Die Norm kann von internen und externen Parteien – darunter Zertifizierungsstellen – dazu eingesetzt werden, die Fähigkeit einer Organisation zur Einhaltung ihrer eigenen Informationssicherheitsanforderungen zu bewerten.

DIN ISO/IEC 27001 beinhaltet Anforderungen an ein ISMS, das mittelbar zur Informationssicherheit beiträgt. Da das Dokument sehr generisch gehalten ist, um auf alle Organisationen unabhängig von Typ, Größe und Geschäftsfeld anwendbar zu sein, haben diese Anforderungen einen niedrigen technischen Detaillierungsgrad, wobei die Anforderungen an die Prozesse wohl definiert sind.

Folgende, in den Abschnitten 4 bis 10 der Norm genannten Anforderungen spiegeln zusammengenommen den **Plan-Do-Check-Act Zyklus** (vgl. Abbildung 1 in Abschnitt 3.3.2.2) wider und müssen von einer Organisation erfüllt werden, um Konformität zur Norm zu erlangen, siehe Tabelle 3:

[19] Siehe https://www.iso.org.
[20] Siehe http://www.iec.ch/.

Abschnitt/ Thema	Subthemen	Erläuterung
4 Kontext der Organisation	4.1 Verständnis der Organisation und ihres Kontextes 4.2 Verständnis der Bedürfnisse und Erwartungen interessierter Parteien 4.3 Festlegung des Geltungsbereichs des ISMS 4.4 ISMS	Definition der Anforderungen, um externe und interne Belange und Wünsche der Beteiligten zu verstehen und den Umfang des ISMS zu definieren
5 Führung	5.1 Führung und Engagement 5.2 Leitlinie 5.3 Organisatorische Aufgaben, Zuständigkeiten und Befugnisse	Festlegung von Rollen und Verantwortlichkeiten, und der Inhalte der obersten IT-Sicherheitsrichtlinien
6 Planung	6.1 Maßnahmen zum Umgang mit Risiken und Chancen 6.2 Informationssicherheitsziele und Pläne für deren Erreichung	Definition der Anforderungen für Risikomanagement, Erklärung zur Anwendbarkeit, und Bestimmung der Ziele der Informationssicherheit
7 Unterstützung	7.1 Ressourcen 7.2 Kompetenz 7.3 Bewusstsein 7.4 Kommunikation 7.5 Dokumentierte Informationen	Anforderungen für das Schutzziel Verfügbarkeit von Ressourcen, Kompetenzen, Bewusstsein, Kommunikation und Kontrolle von Dokumenten und Einträgen
8 Einsatz / Betrieb	8.1 Einsatzplanung und -kontrolle 8.2 Informationssicherheitsrisikoeinschätzung 8.3 Informationssicherheitsrisikobehandlung	Anforderungen an Risikobehandlung und Sicherheitsmaßnahmen
9 Leistungsauswertung	9.1 Überwachung, Messung, Analyse und Auswertung 9.2 Internes Audit 9.3 Prüfung durch die Leitung	Anforderungen für Überwachung, Messung, Analyse und Bewertung, interne Audits und Managementprüfung
10 Verbesserung	10.1 Fehler und Korrekturmaßnahmen 10.2 Laufende Verbesserung	Anforderungen für Abweichungen, Korrekturen, und kontinuierliche Verbesserung

Tabelle 3: Anforderungen des Plan-Do-Check-Act Zyklus

3.3.1.4 ISO 27002

Diese Internationale Norm wurde erarbeitet, um Organisationen als Referenz zur Auswahl von Maßnahmen bei der Einführung eines **Informationssicherheitsmanagementsystems (ISMS)** nach ISO/IEC 27001 zu dienen oder als Leitfaden für Organisationen, die gemeinhin akzeptierte Maßnahmen für die Informationssicherheit einführen möchten. Sie enthält Richtlinien für organisatorische Normen und Managementpraktiken bezüglich Informationssicherheit, einschließlich Auswahl, Implementierung und Management von Sicherheitsmaßnahmen unter Berücksichtigung des Umfelds der Informationssicherheitsrisiken in einer Organisation.

Das Dokument ist gut strukturiert und gliedert sich in 14 Abschnitte („clauses“) über Sicherheitsmaßnahmen („controls“) mit 35 Hauptkategorien („main security categories“) der Sicherheit und 113 Sicherheitsmaßnahmen.

Jede Hauptkategorie von Sicherheitsmaßnahmen enthält:

- Allgemeine Zielsetzung der zugehörigen Sicherheitsmaßnahmen und was erreicht werden soll („control objective“)
- Eine oder mehrere Sicherheitsmaßnahme(n), die zur Erreichung dieser Zielsetzung angewendet werden können.

Die Beschreibungen der Sicherheitsmaßnahmen sind wie folgt strukturiert:

- Maßnahme („control“)
  Definition der spezifischen Sicherheitsmaßnahme und Erklärung, wie das Ziel der Maßnahme erreicht wird.
- Umsetzungshinweise („implementation guidance“)
  Detaillierte (aber weniger detailliert als Grundschutzmaßnahmen des BSI) Information zur Umsetzung von Sicherheitsmaßnahmen und zur Erreichung ihrer Ziele. Es wird ausdrücklich darauf aufmerksam gemacht, dass die Umsetzungshinweise vielleicht nicht in allen Situationen ausreichend sind, möglicherweise nicht die spezifischen Sicherheitsanforderungen einer Organisation erfüllen oder nur eingeschränkt anwendbar sein könnten.
- Weitere zu berücksichtigende Informationen, wie rechtliche Aspekte und Verweise auf andere Normen.

Folgende Abschnitte und Hauptkategorien von Sicherheitsmaßnahmen werden behandelt, siehe Tabelle 4:

Nr.	Abschnitt	Hauptkategorie(n)
5	Sicherheitsleitlinien	• Managementausrichtung zur Informationssicherheit
6	Organisation der Informationssicherheit	• Interne Organisation • Mobilgeräte und Telearbeit
7	Personalsicherheit	• Vor der Anstellung • Während der Anstellung • Beendigung und Wechsel der Anstellung
8	Management von organisationseigenen Werten (assets)	• Verantwortung für organisationseigene Werte • Klassifizierung von Informationen • Handhabung von Speicher- und Aufzeichnungsmedien
9	Zugriffskontrolle	• Geschäftliche Anforderungen in Bezug auf die Zugriffskontrolle • Benutzerverwaltung • Benutzerverantwortung • Kontrolle des Zugangs zu Systemen und Anwendungen
10	Kryptographie	• Kryptographische Maßnahmen
11	Schutz vor physischem Zugang und Umwelteinflüssen	• Sicherheitsbereiche • Sicherheit von Betriebsmitteln
12	Betriebssicherheit	• Betriebsverfahren und Zuständigkeiten • Schutz vor Malware • Backup • Protokollierung und Überwachung • Kontrolle von Betriebssoftware • Technisches Schwachstellenmanagement

Nr.	Abschnitt	Hauptkategorie(n)
		• Auswirkungen von Audits auf Informationssysteme
13	Sicherheit in der Kommunikation	• Netzwerksicherheitsmanagement • Informationsübertragung
14	Anschaffung, Entwicklung und Instandhaltung von Systemen	• Sicherheitsanforderungen für Informationssysteme • Sicherheit in Entwicklungs- und Unterstützungsprozessen • Prüfdaten
15	Lieferantenbeziehungen	• Informationssicherheit bei Lieferantenbeziehungen • Management der Dienstleistungserbringung durch Lieferanten
16	Management von Informationssicherheitsvorfällen	• Management von Informationssicherheitsvorfällen und Verbesserungen
17	Informationssicherheitsaspekte des Betriebskontinuitätsmanagements	• Aufrechterhaltung der Informationssicherheit • Redundanzen
18	Richtlinienkonformität	• Einhaltung gesetzlicher und vertraglicher Anforderungen • Informationssicherheitsprüfungen

Tabelle 4: Abschnitte und Hauptkategorien des ISO/IEC 27002

3.3.1.5 ISO/IEC 27019

Die ISO/IEC TR 27019:2015-03 (DIN SPEC 27019:2015-03) ist eine Erweiterung der Norm ISO/IEC 27002 auf den Bereich der Prozessleit- und Automatisierungstechnik in der Energieversorgung. Sie ergänzt und vertieft dies in Bezug auf Prozesssteuerungssysteme und Netzwerke zur Steuerung und Überwachung von Erzeugung, Übertragung und Verteilung von Strom, Gas und Wärme in Kombination mit der Steuerung von unterstützenden Prozessen. Die Norm ist anwendbar auf Leit- und Automatisierungssysteme, Schutz- und Safetysysteme sowie Messtechnik inklusive der zugehörigen Kommunikations- und Fernwirktechnik.

Folgende Maßnahmen ergänzen die ISO/IEC 27002 hinsichtlich der Erfordernisse im Bereich Energieversorgung (die Nummerierung bezieht sich dabei auf die ISO/IEC 27002:2005), siehe Tabelle 5:

Nr.	Titel	Beschreibung
9.1.7	Sichern von Leitstellen	Maßnahmen zur physischen Sicherheit von Leitstellen mit zentralen Prozesssteuerungssystemen wie Steuerungsservern, MMI-Systemen und unterstützenden Systemen, sollten konzipiert, entwickelt und umgesetzt werden.
9.1.8	Sicherung von Technikräumen	Maßnahmen zur physischen Sicherheit von Technikräumen für Prozesssteuerungssysteme der Energieversorgung sollten konzipiert, entwickelt und umgesetzt werden.
9.1.9	Sicherung von Außenstandorten	Maßnahmen zur physischen Sicherheit von Außenstandorten, an denen Prozesssteuerungssysteme der Energieversorgung betrieben werden, sollten konzipiert, entwickelt und umgesetzt werden.

Nr.	Titel	Beschreibung
9.3.1	Betriebseinrichtung in Bereichen anderer Energieversorger	Wenn Energieversorger Betriebseinrichtungen außerhalb der eigenen Gelände oder Räumlichkeiten in den Verantwortungsbereichen anderer Versorger betreiben, wie beispielsweise in Übergabestationen, sollte die Betriebseinrichtung in einem gesicherten Bereich positioniert werden, so dass die Risiken von umgebungsbezogenen Bedrohungen oder Gefahren und eines nicht autorisierten Zugriffs reduziert werden.
9.3.2	Betriebseinrichtung beim Kunden vor Ort	Wenn Energieversorger Betriebseinrichtungen beim Kunden vor Ort betreiben, z. B. um die Energielieferung zu steuern, zu messen und/oder um zusätzliche Dienste bereitzustellen, sollte die Betriebseinrichtung geschützt werden, so dass die Risiken von umgebungsbezogenen Bedrohungen oder Gefahren und eines nicht autorisierten Zugriffs reduziert werden.
9.3.3	Gekoppelte Steuerungs- und Kommunikationssysteme	Wenn Prozesssteuerungssysteme und zugehörige Kommunikationsverbindungen mit denen von externen Dritten gekoppelt werden, sollten die Verantwortungsgrenzen und Schnittstellen zu allen externen Beteiligten von den Kunden klar definiert und spezifiziert werden, so dass jedes Unternehmen in einem angemessenen Zeitraum abgetrennt und isoliert werden kann, um identifizierte bekannte Risiken abzuwenden.
10.6.3	Sicherung der Prozessdatenkommunikation	Maßnahmen zur Sicherstellung der Vertraulichkeit, Integrität und Verfügbarkeit der internen und externen Prozessdatenkommunikation sollten in Abhängigkeit der Sensibilität der übertragenen Daten konzipiert, entwickelt und umgesetzt werden.
10.11.1	Behandlung von Altsystemen	Alle herkömmlichen Prozesssteuerungssystemtechnologien, Systeme und Komponenten (Legacy-Systeme) sollten mit ihren potentiellen Informationssicherheitsschwachstellen identifiziert werden. Zur Minderung der identifizierten Risiken von alten Prozesssteuerungssystemtechnologien und Prozesssteuerungssystemen sollten entsprechende Maßnahmen umgesetzt werden.
10.12.1	Integrität und Verfügbarkeit von Funktionen der Betriebssicherheit	Die Integrität und Verfügbarkeit von Informationswerten (Information Assets), Systemen, Komponenten und Funktionen, die zur Sicherstellung der Betriebssicherheit (Safety) benötigt werden, sollte im Einklang mit den branchenspezifischen Normen und Gesetzen sichergestellt werden.
11.4.8	Logische Anbindung von externen Prozesssteuerungssystemen	Vor der logischen Kopplung von Prozesssteuerungssystemen und den zugehörigen Kommunikationsverbindungen mit externen Dritten, sollte vom Energieversorger sichergestellt werden, dass ausschließlich erlaubte Kommunikation und Informationsflüsse sowie berechtigte Steuerbefehle und Meldungen über die Kommunikationsverbindung ausgetauscht werden können. Das durch die Kopplung resultierende Risiko sollte entsprechend bewertet werden.
14.2.1	Notfall-Kommunikation	Im Falle von Großstörungen, Naturkatastrophen, Unfällen oder anderen möglichen Notfallsituationen oder wenn das Risiko eines Eintretens eben dieser besteht, sollten Energieversorger sicherstellen, dass wichtige Kommunikationsverbindungen mit dem eigenen Notfallpersonal oder dem

Nr.	Titel	Beschreibung
		Notfallpersonal anderer Versorger, wichtigen Prozesssteuerungssystemen und externen Notfall-Organisationen, die zum Schutz, zur Behandlung oder zur Wiederherstellung nach solchen Vorfällen notwendig sind, zur Verfügung stehen.

Tabelle 5: Ergänzende Maßnahmen der ISO/IEC 27019 in Bezug auf die ISO/IEC 27002

3.3.2 BSI IT-Grundschutz

Zunächst wird ein Überblick über den BSI IT-Grundschutz gegeben. Anschließend wird detailliert auf die Standards, den Katalog und die Profile eingegangen.

3.3.2.1 Einführung in den BSI IT-Grundschutz

Der Kerngedanke des IT-Grundschutzes ist die Vorgabe von Standardsicherheitsmaßnahmen für einen **Informationsverbund** mit normalem Schutzbedarf, ohne dass dafür zunächst eine dedizierte Risikoanalyse durchgeführt werden muss. Es wird angenommen, dass – für bestimmte weit verbreitete Technologien und übliche Einsatzszenarien – den relevanten Gefährdungen durch die Grundschutzmaßnahmen ausreichend begegnet werden kann. Dieses pauschalierte Vorgehen erlaubt zum einen die schnelle Bestimmung der notwendigen Maßnahmen und zum anderen steht ein sehr umfangreicher Fundus an detailliert ausformulierten Standardmaßnahmen aus den Bereichen Infrastruktur, Organisation, Personal, Hardware, Software, Netze und Notfallvorsorge zur Verfügung.

Im Bearbeitungszeitraum der AS12.2.1 und 12.2.4 bestand der BSI IT-Grundschutz zunächst aus den seit 2006 bzw. 2008 geltenden BSI-Standards

- 100-1: Managementsysteme für Informationssicherheit
- 100-2: IT-Grundschutz-Vorgehensweise
- 100-3: Risikoanalyse auf der Basis von IT-Grundschutz
- 100-4: Notfallmanagement

sowie den IT-Grundschutzkatalogen, Stand 15. Ergänzungslieferung.

Diese Dokumente enthielten Empfehlungen des BSI zu Methoden, Prozessen und Verfahren sowie Vorgehensweisen und Maßnahmen mit Bezug zur Informationssicherheit.

Im Jahr 2017 wurde der IT-Grundschutz modernisiert, und seit April 2017 liegen die aktualisierten Standards 200-1 bis 200-3 vor.

- **BSI-Standard 200-1** definiert allgemeine Anforderungen an ein Managementsystem für Informationssicherheit (ISMS). Er ist weiterhin kompatibel zum ISO-Standard 27001 und berücksichtigt die Empfehlungen der anderen ISO-Standards wie beispielsweise ISO 27002.
- **BSI-Standard 200-2** bildet die Basis der bewährten BSI-Methodik zum Aufbau eines soliden Informationssicherheitsmanagements (ISMS). Er etabliert drei neue Vorgehensweisen bei der Umsetzung des IT-Grundschutzes.

- Der **BSI-Standard 200-3** beinhaltet erstmals gebündelt alle risikobezogenen Arbeitsschritte bei der Umsetzung des IT-Grundschutzes. Der Vorteil für die Anwender ist ein deutlich reduzierter Aufwand, um ein angestrebtes Sicherheitsniveau zu erreichen. Der Standard bietet sich an, wenn Unternehmen oder Behörden bereits erfolgreich mit der IT-Grundschutz-Methodik arbeiten und möglichst direkt eine Risikoanalyse an die IT-Grundschutz-Analyse anschließen möchten." [BSI 18]

Zur Ablösung der bisherigen Standards schreibt das BSI als Herausgeber: „Die Umstellung auf den modernisierten IT-Grundschutz hat Auswirkungen auf ein Managementsystem für Informationssicherheit (ISMS), das nach der bisherigen IT-Grundschutz-Methode gemäß BSI-Standard BSI 100-2 und den IT-Grundschutz-Katalogen aufgebaut ist. Damit betrifft die Umstellung vor allem zertifizierte und nicht-zertifizierte Institutionen. Den IT-Grundschutz-Anwendern stellt das BSI zur erfolgreichen Migration eine „Anleitung zur Migration von Sicherheitskonzepten" zur Verfügung. Anhand dieser und der darüber hinaus veröffentlichten Migrationstabellen können Anwender bestehende Sicherheitskonzepte auf der Basis des „alten" IT-Grundschutzes effektiv auf den modernisierten IT-Grundschutz migrieren." [BSI 18]

Der **Standard 100-4** zum Notfallmanagement blieb bisher bestehen. Der bisher noch nicht veröffentlichte **Standard 200-4** wird den Fokus auf das gesamte Business Continuity Management erweitern und die Möglichkeit der stufenweisen Einführung eines solchen unterstützen[21].

Die BSI IT-Grundschutzkataloge mit Bausteinen und Sicherheit*smaßnahmen* wurden vom IT-Grundschutzkompendium abgelöst, das ebenfalls Bausteine sowie jeweils Baustein-spezifische Sicherheits*anforderungen* enthält. Zu den Sicherheitsanforderungen wurden teilweise bereits zugehörige Umsetzungshinweise bereitgestellt.

Seit dem 1. Februar 2018 dient das IT-Grundschutz-Kompendium als Prüfgrundlage für Zertifizierungen nach ISO 27001 auf Basis von IT-Grundschutz.

Das IT-Grundschutz-Kompendium wurde im Februar 2020 in der 3. Edition 2020 veröffentlich. Weiteres hierzu siehe Kapitel 3.3.2.6

3.3.2.2 BSI-Standard 200-1: Managementsysteme für Informationssicherheit (ISMS)

„Der im Rahmen der IT-Grundschutz-Modernisierung aktualisierte BSI-Standard 200-1 definiert allgemeine Anforderungen an ein Managementsystem für Informationssicherheit (ISMS). Er ist weiterhin kompatibel zum ISO-Standard 27001 und berücksichtigt die Empfehlungen der anderen ISO-Standards wie beispielsweise ISO 27002. Die leicht verständliche und systematische Anleitung zum Aufbau eines ISMS ist dabei unabhängig von der eingesetzten Methode. Die Struktur des Standards 200-1 ist so konzipiert, dass sie zur IT-Grundschutz-Vorgehensweise kompatibel ist.

[21] Siehe hierzu z. B. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BCM/BCM_20190416_Infomail.html

Im Hinblick auf die fachliche Auseinandersetzung mit der gesamten IT-Grundschutz-Methodik ist der aktualisierte BSI-Standard 200-1 am BSI-Standard 200-2 zur IT-Grundschutz-Vorgehensweise ausgerichtet sowie an der überarbeiteten ISO 27001:2013. Aufgrund der ähnlichen Struktur der beiden Standards 200-1 und 200-2 können Anwender sich gut in beiden Dokumenten zurechtfinden“ [BSI 18]

Der Standard beschreibt, wie ein Informationssicherheitsmanagementsystem (ISMS) grundsätzlich in einer Organisation aufgebaut werden kann. Der PDCA-Zyklus (Plan, Do, Check Act) wird erläutert (siehe Abbildung 1).

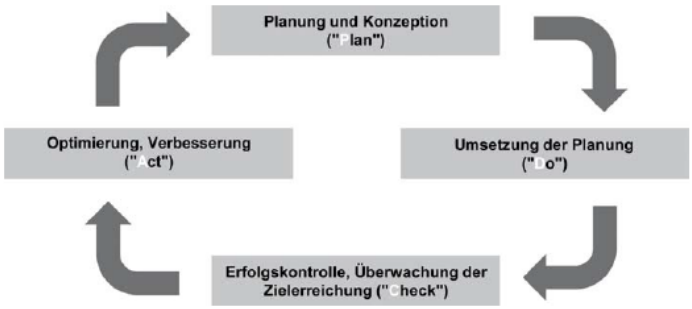


Abbildung 1: PDCA-Zyklus (Quelle: BSI-Standard 100-1)

Weitere wesentliche Elemente und Grundbegriffe eines ISMS werden erläutert und in Zusammenhang gebracht. Darunter fallen die Themen:

- Standards zur Informationssicherheit
- Informationssicherheitsprozess
- Informationssicherheitsorganisation
- Sicherheitskonzept
- Managementprinzipien
- Ressourcen für Informationssicherheit
- Leitlinie zur Informationssicherheit

3.3.2.3 BSI-Standard 200-2: IT-Grundschutz-Methodik

Die IT-Grundschutz-Vorgehensweise beschreibt Schritt für Schritt, wie ein Managementsystem für Informationssicherheit in der Praxis aufgebaut und betrieben werden kann. Die Aufgaben des Informationssicherheitsmanagements und der Aufbau einer Organisationsstruktur für Informationssicherheit sind dabei wichtige Themen. Die IT-Grundschutz-Vorgehensweise geht sehr ausführlich darauf ein, wie ein Sicherheitskonzept in der Praxis erstellt werden kann, wie angemessene Sicherheitsmaßnahmen ausgewählt werden können und was bei der Umsetzung des Sicherheitskonzeptes zu beachten ist.

Der BSI-Standard 200-2 löste im Oktober 2017 den BSI-Standard 100-2 ab. Im Rahmen der Modernisierung des IT-Grundschutzes wurden neben der Standard-Absicherung, welche im Wesentlichen der allgemeinen IT-Grundschutzvorgehensweise des bisherigen BSI-Standard 100-2 entspricht, die Vorgehensweisen zur Basis-Absicherung und zur Kern-Absicherung hinzugefügt.

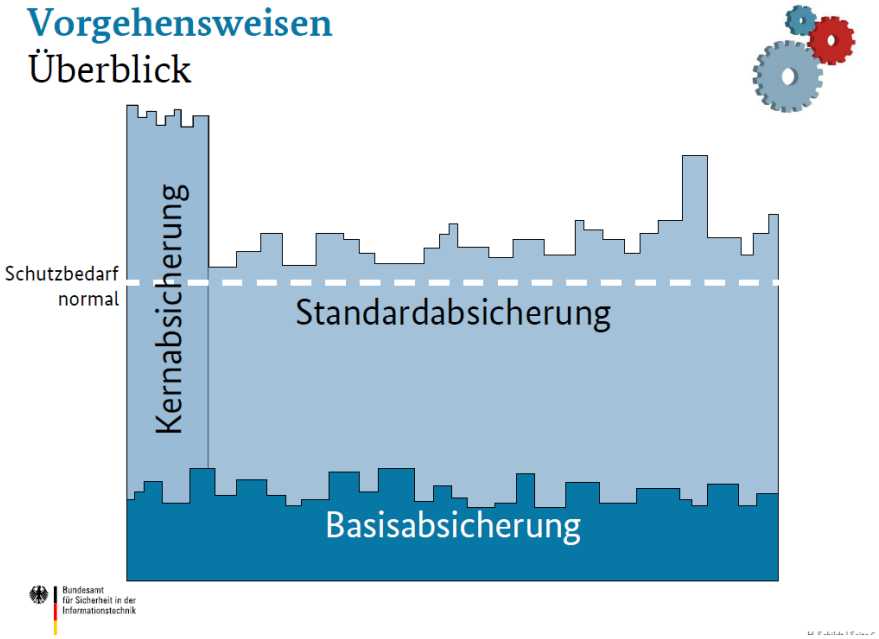
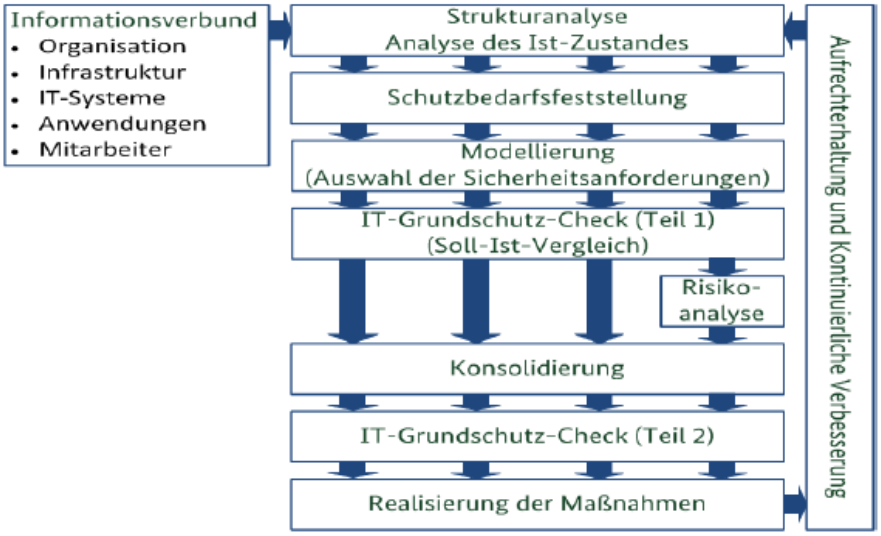


Abbildung 2: Vorgehensweisen nach IT-Grundschutz (BSI)

Weitere Neuerungen sind:

- Wegfall der ergänzenden Sicherheitsanalyse als eigener Schritt der Grundschutzmethodik
- Erweiterung um Virtualisierung, Cloud-, Industrial-Control-Systems- (ICS) und Internet-of-Things- (IoT) -Absicherung
- Klarstellung der Rollen und Aufgaben von IT-Sicherheitsbeauftragten (IT-SiBe) und Informationssicherheitsbeauftragten (ISB)
- Anpassungen an Fortschreibung der ISO-Standards
- Betonung der Informationsklassifizierung
- Überarbeitung des Informationsflusses im Informationssicherheitsprozess, Angleichung mit BSI-Standard 100-4



Quelle: BSI 200-2

Abbildung 3: Erstellung eines IT-Sicherheitskonzepts mit der Standard-Absicherung (BSI-Standard 200-2)

Die einzelnen Schritte der Standardabsicherung umfassen:

1. Festlegen des Informationsverbundes

Ein Informationsverbund soll alle organisatorischen Maßnahmen, personellen Ressourcen sowie technischen und infrastrukturellen Komponenten umfassen, die zur Unterstützung einer oder mehrerer Fachaufgaben, Geschäftsprozesse oder Organisationseinheiten dienen.

2. Strukturanalyse

Bei der Strukturanalyse geht es um die Erfassung der Bestandteile (Geschäftsprozesse, Informationen, Anwendungen, IT-und ICS-Systeme, Räume, Kommunikationsnetze), die zur Betrachtung des Geltungsbereichs benötigt werden.

Dazu gehören auch eine Netzplanerhebung und die Komplexitätsreduktion durch Gruppenbildung. Die Strukturanalyse dient der Erhebung von Informationen, die für die weitere Vorgehensweise in der Erstellung eines Sicherheitskonzepts nach ISO 27001 / IT-Grundschutz benötigt werden.

3. Feststellung des Schutzbedarfs

In der Schutzbedarfsfeststellung wird nach der Definition der Schutzbedarfskategorien für die bei der Strukturanalyse erfassten Objekte im Informationsverbund entschieden, welchen Schutzbedarf sie bezüglich der Vertraulichkeit, Integrität und Verfügbarkeit besitzen. Dieser Schutzbedarf orientiert sich an den möglichen Schäden, die mit einer Beeinträchtigung der betroffenen Anwendungen und damit der jeweiligen Geschäftsprozesse verbunden sind.

4. Modellierung nach IT-Grundschutz

Die Modellierung besteht darin, Zielobjekten bzw. Gruppen von Zielobjekten Bausteine des IT-Grundschutz-Kompendiums (siehe Kapitel 3.3.2.6) zuzuordnen.

Das IT-Grundschutz-Modell eines *bereits realisierten* Informationsverbunds identifiziert über die verwendeten Bausteine die relevanten Sicherheitsanforderungen. Es kann in Form eines Prüfplans benutzt werden, um einen Soll-Ist-Vergleich durchzuführen.

Das IT-Grundschutz-Modell eines *geplanten* Informationsverbunds stellt hingegen ein Entwicklungskonzept dar. Es beschreibt über die ausgewählten Bausteine, welche Sicherheitsanforderungen bei der Realisierung des Informationsverbunds erfüllt werden müssen.

5. IT-Grundschutz-Check

Beim IT-Grundschutz-Check (Soll-Ist-Vergleich) wird die vorliegende Modellierung nach IT-Grundschutz als Prüfplan benutzt, um nach organisatorischen Vorarbeiten (Sichtung relevanter hausinterner Papiere, z. B. Organisationsverfügungen, Arbeitshinweise, Sicherheitsanweisungen, Handbücher; Ermittlung geeigneter Interviewpartner, Entscheidung über die Beteiligung Externer) anhand eines Soll-Ist-Vergleichs herauszufinden, welche Anforderungen bereits ausreichend oder welche bisher nur unzureichend erfüllt wurden.

6. Risikoanalyse

Die Risikoanalyse auf der Basis von IT-Grundschutz ist eine Vorgehensweise, um bei Bedarf Sicherheitsvorkehrungen zu ermitteln, die über die im IT-Grundschutz-Kompendium genannten Sicherheitsanforderungen hinausgehen. Dies ist insbesondere dann erforderlich, wenn

- die Schutzbedarfskategorie "hoch" oder "sehr hoch" in mindestens einem der Grundwerte vorliegt,
- zusätzlicher Analysebedarf besteht (z. B. bei besonderem Einsatzumfeld) oder
- für bestimmte Komponenten oder Aspekte kein geeigneter Baustein im IT-Grundschutz-kompendium vorhanden ist.

Bei der Umsetzung der Sicherheitskonzeption werden die zu erfüllenden *Anforderungen* aus den IT-Grundschutz-Bausteinen passend zu den organisatorischen und technischen Gegebenheiten der Institution zu *Sicherheitsmaßnahmen* konkretisiert. Die *Umsetzungshinweise* des IT-Grundschutzes geben dazu für viele Bausteine und Anforderungen praxisnahe Empfehlungen.

3.3.2.4 RBSI-Standard 200-3: Risikoanalyse auf der Basis von IT-Grundschutz

Der BSI-Standard 200-3 beschäftigt sich mit dem Risikomanagement.

„Im BSI-Standard 200-3 sind erstmals alle risikobezogenen Arbeitsschritte bei der Umsetzung des IT-Grundschutzes gebündelt dargestellt. Der Vorteil für die Anwender ist ein deutlich reduzierter Aufwand, um ein angestrebtes Sicherheitsniveau zu erreichen. Der Standard bietet sich an, wenn Unternehmen oder Behörden bereits erfolgreich mit der IT-Grundschutz-Methodik arbeiten und möglichst direkt eine Risikoanalyse an die IT-Grundschutz-Analyse anschließen möchten. Die Risikoanalyse aus dem bisherigen BSI-Standard 100-3 wurde in ein vereinfachtes Gefährdungsmodell überführt.“ [BSI 18]

Aufbauend auf der durchgeführten ergänzenden Sicherheitsanalyse und der damit einhergehenden Managemententscheidung für die in Frage kommenden Zielobjekte wird wie schon nach Standard 100-3 eine Risikoanalyse durchgeführt, mit den Schritten:

- Gefährdungsübersicht
- Zusätzliche Gefährdungen
- Gefährdungsbewertung
- Risikobehandlung
- Konsolidierung

Die wesentlichen Neuerungen des Standard 200-3 betreffen:

- Umstellung der Risikoanalyse, jetzt auf Basis der elementaren Gefährdungen,
- Einführung Risikomanagementsystem,
- Einführung Matrix-Ansatz zur Bewertung von Risiken,
- Einführung Risikoappetit und Chancenmanagement.

Die Einordnung der Risikoanalyse in den Sicherheitsprozess ist Abbildung 4 zu entnehmen.

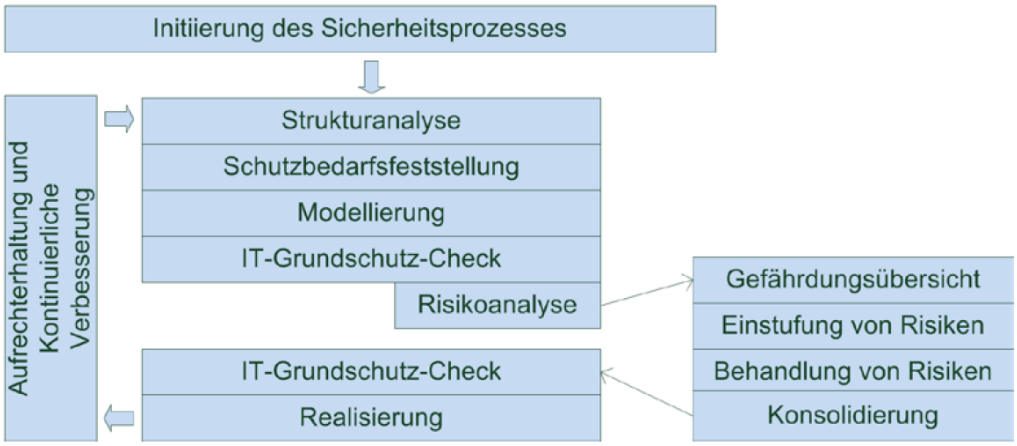


Abbildung 4: Einordnung der Risikoanalyse in den Sicherheitsprozess (Quelle: BSI-Standard 200-3)

3.3.2.5 BSI-Standard 100-4 Notfallmanagement

Mit dem BSI-Standard 100-4 wird ein systematischer Weg aufgezeigt, ein Notfallmanagement in einer Behörde oder einem Unternehmen aufzubauen, um die Kontinuität des Geschäftsbetriebs sicherzustellen. Aufgaben eines Notfallmanagements sind daher, die Ausfallsicherheit zu erhöhen und die Institution auf Notfälle und Krisen adäquat vorzubereiten, damit die wichtigsten Geschäftsprozesse bei Ausfall schnell wieder aufgenommen werden können. Es gilt, Schäden durch Notfälle oder Krisen zu minimieren und die Existenz der Behörde oder des Unternehmens auch bei einem größeren Schadensereignis zu sichern.

Der Standard BSI-Standard 100-4 ist relativ komplex und seine Umsetzung ist mit recht hohem Aufwand verbunden. Deshalb hat das BSI im Nachgang ein „Umsetzungsrahmenwerk zum Notfallmanagement nach BSI-Standard 100-4“ herausgegeben.

Der Standard 100-4 zum Notfallmanagement befindet sich auch Ende 2020 noch in der Überarbeitung. Die Neufassung als Standard 200-4 wird voraussichtlich entsprechend einem etwas erweiterten Blickwinkel die Bezeichnung „Business Continuity Management“ erhalten.

Neben inhaltlichen Aktualisierungen ist die Neueinführung eines Stufenmodells vorgesehen, das den Einstieg einer Institution in das Notfallmanagement bzw. in das BCM durch Zwischenstufen erleichtern soll, in denen zunächst nur eine eingeschränkte Anzahl an Prozessen einbezogen wird, und bzw. oder eine vereinfachte Methodik angewandt wird, bevor ein vollumfängliches Notfallmanagement bzw. BCM etabliert wird. Angaben zum aktuellen Stand finden sich auf der Homepage des BSI[22].

3.3.2.6 IT-Grundschutzkompendium

[22] Der Planungsstand von April 2019, in dem das zukünftig vorgesehene stufenweise Vorgehen beschrieben ist, ist hier zu finden: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BCM/BCM_20190416_Infomail.pdf.
Der z. Zt. aktuellste Bericht zum Stand der Weiterentwicklung von Dezember 2019 ist hier zu finden: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BCM/BCM_20191218_Infomail.pdf

Das IT-Grundschutz-Kompendium ist neben den BSI-Standards die grundlegende Veröffentlichung des IT-Grundschutzes. Das umfangreiche Arbeitsinstrument und Nachschlagewerk zur Informationssicherheit enthielt in der 1. Edition 2018 die ersten 80 IT-Grundschutz-Bausteine, die in den folgenden Editionen kontinuierlich aktualisiert und erweitert wurden und werden.

Das IT-Grundschutz-Kompendium löste die IT-Grundschutzkataloge ab[23], die die BSI-Standards 100-1 bis 100-3 ergänzten. „Die Umstellung auf den modernisierten IT-Grundschutz hat Auswirkungen auf ein Managementsystem für Informationssicherheit (ISMS), das nach der bisherigen IT-Grundschutz-Methode gemäß BSI-Standard BSI 100-2 und den IT-Grundschutz-Katalogen aufgebaut ist.“ [BSI 18]. Das BSI unterstützt Anwender bei der Umstellung mit einer Anleitung zur Migration von Sicherheitskonzepten und Migrationstabellen.

Die Bausteine im IT-Grundschutz-Kompendium sind zum Teil Fortschreibungen von Bausteinen aus dem alten IT-Grundschutz, viele Bausteine sind jedoch im Zuschnitt geändert oder ganz neu. Im IT-Grundschutz-Kompendium sind diese Bausteine nach zehn Schichten strukturiert, die wiederum in einzelne Prozess- und Systembausteine unterteilt sind:

Prozessbausteine

- CON - Konzepte & Vorgehensweisen
- DER - Detektion & Reaktion
- ISMS - Sicherheitsmanagement
- OPS - Betrieb
- ORP - Organisation & Personal

Systembausteine

- APP – Anwendungen
- IND - Industrielle IT
- INF - Infrastruktur
- NET - Netze
- SYS - IT-Systeme

Jeder Baustein enthält spezifische Gefährdungen und Sicherheitsanforderungen (keine Maßnahmen mehr) für den jeweiligen Bereich. Die Sicherheitsanforderungen sind deutlich kürzer formuliert als die bisherigen Sicherheitsmaßnahmen, und sie schreiben auch nicht mehr explizit vor, wie ein bestimmtes Sicherheitsziel erreicht werden muss.

Um dennoch auf die gewaltige Wissensbasis, welche die bisherigen Maßnahmen darstellen nicht verzichten zu müssen, gibt bereits zu zahlreichen Bausteinen Umsetzungshinweise, in denen zu den Anforderungen die passenden Sicherheitsmaßnahmen aufgezeigt werden, also wie etwas getan werden kann.

[23] In Einzelfällen können die Inhalte der IT-Grundschutzkataloge vorerst weiterhin von Nutzen sein, z. B. wenn die Entsprechung eines Bausteins der IT-Grundschutzkataloge im neuen IT-Grundschutz-Kompendium noch nicht enthalten ist. Dort wo es zu den Anforderungen des IT-Grundschutz-Kompendiums noch keine Umsetzungshinweise gibt, können ggf. Maßnahmen aus den IT-Grundschutzkatalogen herangezogen werden.

Die Anforderungen der Bausteine sind in drei Kategorien gegliedert: Basis- und Standard-Anforderungen sowie Anforderungen für einen höheren Schutzbedarf. Vorrangig sollten die Basis-Anforderungen umgesetzt werden, da sie mit geringem Aufwand den größtmöglichen Nutzen erzielen. Darauf aufbauend vervollständigen die Standard-Anforderungen den Stand der Technik und adressieren den normalen Schutzbedarf. Ergänzend dazu enthalten die modernisierten Bausteine Beispiele für Sicherheitsanforderungen bei hohem Schutzbedarf.

Die aktuelle 3. Edition 2020 des IT-Grundschutz-Kompendium enthält nicht nur einzelne neue Bausteine, sondern auch weitere Änderungen[24]: Neben der sprachlichen und inhaltlichen Überarbeitung hat das BSI auch zahlreiche strukturelle Verbesserungen an den IT-Grundschutz-Bausteinen vorgenommen. Diese sollen Redundanzen vermindern und klarere Abgrenzungen schaffen, um es den Anwendern zu ermöglichen, die Bausteine noch gezielter einzusetzen – sowohl bei der Anwendung einzelner Bausteine als auch in Kombination.

Die wichtigsten Änderungen sind diese:

- In jedem Baustein finden sich jetzt auch explizite Hinweise zum Einsatz bei der Modellierung, z. B. für welche Zielobjekte er anzuwenden ist, und durch welche anderen Bausteine er zu ergänzen ist sowie welcher Baustein ggf. alternativ zu verwenden ist.
- In Bezug auf den Standard 200-2 wird die Zuständigkeit einzelner Rollen stärker hervorgehoben
- Viele Bezeichnungen von Anforderungen (Anforderungstitel) wurden präzisiert.
- In den Kreuzreferenztabellen, die pro Baustein die Elementaren Gefährdungen und die Anforderungen in Beziehung zueinander setzen, werden nun auch zunehmend Angaben dazu aufgenommen, welche Grundwerte durch eine Anforderung vorrangig geschützt werden, so dass in einer Kreuzreferenztabelle alle Aspekte zur Risikoanalyse gebündelt sind.

3.3.2.7 IT-Grundschutz-Profile im modernisierten IT-Grundschutz

IT-Grundschutz-Profile sind als Schablonen zu verstehen, mit denen verschiedene Anwender(-gruppen) selbstständig den IT-Grundschutz auf ihre Bedürfnisse anpassen können. Beispielsweise ist es denkbar, dass z. B. mehrere kleine Institutionen, Kommunalverwaltungen, Krankenhäuser oder Betreiber kritischer Infrastrukturen zentral definieren, welche Empfehlungen für sie essenziell, optional oder verzichtbar sind.

„Unternehmen oder Behörden können IT-Grundschutz-Profile für bestimmte Anwendungsfälle erstellen und im Anschluss weiteren Interessierten zur Verfügung stellen. Anwender, die ähnliche Sicherheitsanforderungen haben, können anhand dieser Vorlage ressourcenschonend das Sicherheitsniveau überprüfen oder damit beginnen, ein Managementsystem für Informationssicherheit (ISMS) nach IT-Grundschutz aufzubauen. Ziel ist es, dass perspektivisch ein breites Portfolio von IT-Grundschutz-Profilen als Musterszenarien für unterschiedliche Anwendungsfelder zur Verfügung gestellt wird. Weitere Anwender können durch die Arbeit mit den

[24] Siehe hierzu auch die Übersicht aller Änderungen in der Edition 2020 relativ zur vorausgehenden Edition 2019 auf der Website des BSI: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/FD_Aenderungen2020.html

IT-Grundschutz-Profilen den zeitlichen und personellen Aufwand deutlich reduzieren, indem sie die Sicherheitsbetrachtungen auf die individuellen Rahmenbedingungen übertragen. In einem IT-Grundschutz-Profil werden die einzelnen Schritte eines Sicherheitsprozesses für einen definierten Anwendungsbereich dokumentiert, dazu gehören:

- Festlegung des Anwendungsbereichs
- Durchführung einer verallgemeinerten Strukturanalyse, Schutzbedarfsfeststellung und Modellierung für diesen Bereich
- Auswahl und Anpassung von umzusetzenden IT-Grundschutz-Bausteinen sowie Beschreibung spezifischer Sicherheitsanforderungen und -maßnahmen.

IT-Grundschutz-Profile sind besonders für Branchen, Sektoren oder andere große Verbünde von Institutionen mit ähnlichen Bedingungen geeignet. Veröffentlicht zum Beispiel ein Maschinenhersteller, eine Zahnarztpraxis oder ein Handwerksbetrieb ein IT-Grundschutz-Profil, so besteht für eine große Anzahl weiterer Betriebe die Möglichkeit, auch ihre IT und ihr Informationsmanagement auf dieser Basis abzusichern. Ein einzelnes IT-Grundschutz-Profil kann dadurch mit der Zeit weiter ergänzt und verbessert werden.“ [BSI 18]

Das BSI hat eine „Anleitung zur Erstellung eines IT-Grundschutz-Profils“ (Strukturbeschreibung) veröffentlicht, die die Anwender durch den gesamten Profilprozess führt[25]. [BSI 18]

Die Übersicht veröffentlichter IT-Grundschutz-Profile[26] [BSI 18] enthält z. Zt. neun Einträge, darunter solche für Papierfabriken, Reedereien und Handwerkskammern, sowie u. a. auch

- IT-Grundschutzprofil für Handwerksbetriebe (Herausgeber: Zentralverband des Deutschen Handwerks (ZDH), Version 1.0 von 2019)
- IT-Grundschutz-Profil: Basis-Absicherung Kommunalverwaltung (Autor: Kommunale Arbeitsgruppe „Modernisierung IT-Grundschutz“, Version 2.0 von 2019)
- IT-Grundschutz-Profil für einen großen IT-Dienstleister (Autor: Christoph Möhring, Working Draft (WD) von 2018)
- Masterarbeit: Erstellung eines IT-Grundschutz-Profils für ein Referenzunternehmen mit automatisierter Prozesssteuerung (Autorin: Sarah Fluchs, Research Group IT-Security RWTH Aachen, 2017)

3.3.3 BDEW Whitepaper Aktualisierung 15.5.2018 IABG

Das BDEW Whitepaper mit dem Titel „Anforderungen an sichere Steuerungs- und Telekommunikationssysteme“[27] wurde durch den Bundesverband der Energie- und Wasserwirtschaft

[25] Aktuellste Informationen siehe unter https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzProfile/Anleitung/itgrundschutzProfile_Anleitung_node.html
[26] Aktueller Stand siehe unter https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzProfile/Profile/itgrundschutzProfile_Profile_node.html
[27] Siehe https://www.bdew.de/service/anwendungshilfen/whitepaper-anforderungen-sichere-steuerungs-telekommunikationssysteme/

(BDEW) in deutscher und englischer Sprache verfasst. Es befasst sich mit den drei Haupttechnologien „Betriebsführungs-/Leitsysteme und Systembetrieb“, „Übertragungstechnik/Sprachkommunikation“ und „Sekundär-, Automatisierungs- und Fernwirktechnik“.

Das Whitepaper soll Unternehmen dabei unterstützen deren Systeme mit niedrigem oder mittlerem Schutzbedarf vor Sicherheitsbedrohungen im täglichen Betrieb zu schützen, indem festgelegte Sicherheitsmaßnahmen realisiert werden. Bei hohem oder sehr hohem Schutzbedarf muss zusätzlich eine gesonderte Risikoanalyse erfolgen. Weiterhin soll Informationssicherheit bereits in der Planungsphase integriert und insgesamt ein gemeinsames Verständnis in der Branche für Informationssicherheit etabliert werden. Zu dem Whitepaper gibt es eine Tabelle[28] mit allen Sicherheitsmaßnahmen als Anwendungshilfe. Zusammen können diese als Management-/Monitoring-Tool für die Einhaltung und Entwicklung der Sicherheitsmaßnahmen verwendet werden.

Das Whitepaper liegt aktuell in der Version 2.0 vom Mai 2018 vor, nachdem es grundlegend durch BDEW und Österreich Energie aktualisiert wurde, wobei die vorher separat veröffentlichten zugehörigen Ausführungshinweise integriert wurden. Die Inhalte wurden entsprechend aktueller Technologien angepasst und ergänzt, wie z. B. zu Cloud-Diensten und Virtualisierungstechnologien. Ferner gibt es Neuerungen in Bezug auf gesetzliche und regulatorische Anforderungen, beispielsweise das IT-Sicherheitsgesetz, die EU NIS Richtlinie (EU-Cybersicherheitsrichtlinie) sowie die EU Datenschutzgrundverordnung. Bei der Neuauflage wurden Branchenerfahrungen sowohl aus Deutschland als auch aus Österreich berücksichtigt.

3.3.4 IEC 62351

Die technische Norm IEC 62351 mit dem ins Deutsche übersetzten Titel „Netzführungssysteme und ihr Informationsaustausch - IT Sicherheit“, beschäftigt sich mit IT-Sicherheit und besonders mit Ende-zu-Ende-Sicherheit für Netzführungssysteme. Dieser Standard hat das Ziel eine sichere Kommunikation von Kontrollsystemen im Umfeld der Energiesystemautomation zu definieren. Die IEC 62351 wird von der internationalen Arbeitsgruppe 15 des Technischen Komitees 57 (TC57 WG15) erarbeitet und ist ein Querschnittsstandard zur Informationssicherheit, der sich über alle Ebenen der SIA[29] (Seamless Integration Architecture) erstreckt. Er übernimmt die Spezifikation von Sicherheitserweiterungen für die im TC57 entwickelten Kommunikationsprotokolle. In Abbildung 5 sind die einzelnen Teile des Standards, in Gelb dargestellt, und deren Abhängigkeiten untereinander sowie zu den entsprechenden Kommunikationsstandards, in Grün dargestellt, zu erkennen.

[28] Sie kann am gleichen Ort heruntergeladen werden wie das Whitepaper
[29] Die SIA ist eine Referenzarchitektur notwendiger Standards für die Umsetzung eines Smart Grids und wird im Standard IEC 62357 definiert.

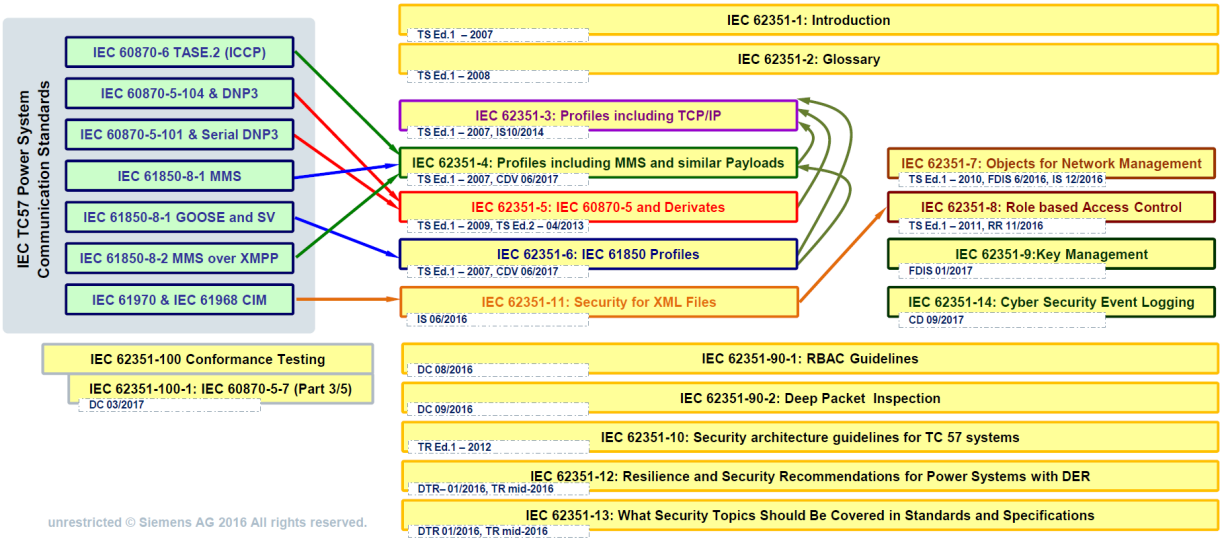


Abbildung 5: Darstellung der Korrelationen zwischen dem IEC 62351 und den verschiedenen Profilen (Quelle: Steffen Fries, Siemens)

Im Folgenden eine kurze Aufzählung der einzelnen Teile der IEC 62351-Standardserie, einzelne Teile sind noch nicht finalisiert oder befinden sich in der Überarbeitung.

- IEC 62351-1, -2: Teil 1 gibt eine Einführung zum Thema und Teil 2 ein Glossar.
- IEC 62351-3, -4, -5 und -6: Teil 3 bis 6 beschreiben Informationssicherheit für verschiedene Profile. Teil 3 für die Internetprotokollfamilie TCP/IP, Teil 4 für MMS-basierte Protokolle, Teil 5 für IEC 60870-5 basierte Protokolle und Teil 6 für IEC 61850 basierte Protokolle.
- IEC 62351-7: Teil 7 behandelt Informationssicherheit für NSM30-Datenobjektmodelle.
- IEC 62351-8: Teil 8 beschreibt eine rollenbasierte Zugriffskontrolle (RBAC) für Leitsysteme.
- IEC 62351-9: Teil 9 erläutert das Schlüsselmanagement im Smart Grid.
- IEC 62351-90-1: Teil -90-1 gibt einen Leitfaden, wie RBAC angewendet werden kann, insbesondere verbraucherbasierte Rollen.
- IEC 62351-90-2: Teil 90-2 beschreibt einen Leitfaden, wie Deep packet inspection bei verschlüsselter Kommunikation ermöglicht werden kann.
- IEC 62351-10: Teil 10 ist eine Richtlinie für Sicherheitsarchitekturen.
- IEC 62351-11: Teil 11 beschäftigt sich mit Informationssicherheit für XML-Dateien.
- IEC 62351-12: Teil 12 gibt Empfehlungen für Ausfall- und Informationssicherheit zwischen dezentralen Energieressourcen (DER).
- IEC 62351-13: Teil 13 ist eine Richtlinie für die Abdeckung von Sicherheitsthemen durch Standards und Spezifikationen im Stromsektor.
- IEC 62351-14: Teil 14 definiert das Event Logging für Cyber Security für Fehleranalysen und Auditing.

[30] NSM steht für Netzwerk- und Systemmanagement.

- IEC 62351-100, -100-1: Teil 100 dient als Mantel/Schirmstandard dazu Entwicklern zu helfen standardkonforme Funktionalitäten anzubieten. Aktuell sind bisher in Teil 100-1 Testfälle für den Teil 5 des IEC 62351 definiert.

3.3.5 IEC 62443

Der IEC 62443 ist eine Informationssicherheitsstandardreihe für die Automatisierungsindustrie mit dem Titel „Industrielle Kommunikationsnetze - IT-Sicherheit für Netze und Systeme“. Diese Reihe unterteilt sich in vier Themen: allgemeine Vorgaben, Regelwerke und Vorgehensweisen, Vorgaben für das Gesamtsystem sowie Vorgaben für einzelne Komponenten (General, Policies and procedures, System, Component). Diese Themen unterteilen sich in weitere Standardteile, wie in Abbildung 6 dargestellt ist.

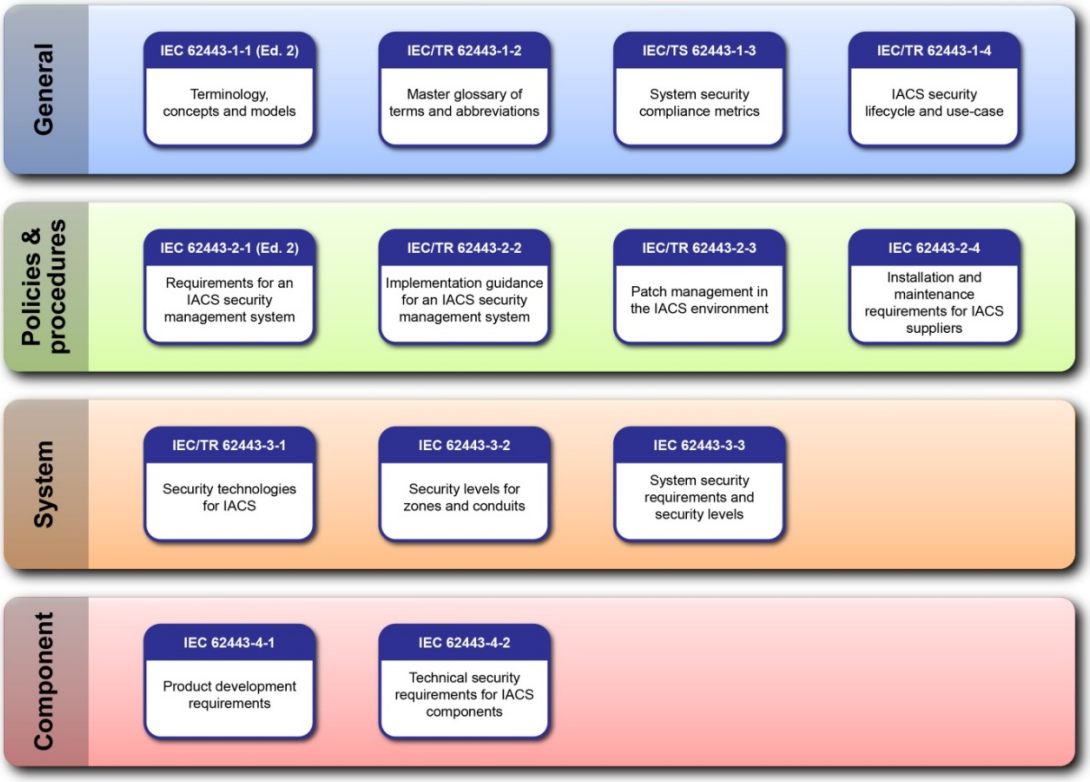


Abbildung 6: Übersicht Normenreihe IEC 62443 (Quelle: www.dke.de)

3.3.6 NISTIR 7628[31]

Das NIST (National Institute for Standards and Technology) ist eine sogenannte nicht-regulative Bundesbehörde innerhalb des US-Wirtschaftsministeriums. Das IR steht für Interagency Report beziehungsweise Internal Report.[32] Als Ergänzung zu der Roadmap für das Smart Grid wurde die NISTIR 7628-Richtlinien entwickelt, die einen Leitfaden für Informationssicherheit

[31] Die NISTIR 7628-Richtlinie kann unter https://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.7628r1.pdf abgerufen werden.

[32] Siehe auch http://csrc.nist.gov/publications/PubsNISTIRs.html.

im Rahmen des Smart Grid beschreiben. Diese Richtlinien beginnen mit einer allgemeinen Einführung in die Thematik, die außerdem die Entwicklungsmethodik der Richtlinien beschreibt. Danach unterteilen sie sich in die folgenden drei Hauptdokumente:

Volume 1 mit dem Titel „Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements“ beschreibt die genutzte Methode zur Identifikation von High-Level Security Anforderungen. Es werden Informationen zum Smart Grid und zu Cyber Sicherheitsstrategien vorgestellt. Das Ziel ist es, die Zuverlässigkeit des Netzes und die Vertraulichkeit von sensiblen Daten zu gewährleisten. Ein High-Level Diagramm wird vorgestellt. Es dient dazu, die Akteure in den Domänen zu verorten. Darauf aufbauend entsteht ein übergreifendes Referenzmodell. Durch dieses werden 22 logische Interface-Kategorien – innerhalb und übergreifend über sieben Smart Grid Domänen – identifiziert und definiert. Daraus werden die sogenannte Smart Grid Cyber Security Requirements abgeleitet. Volume 2 mit dem Titel „Privacy and the Smart Grid“ betrachtet verschiedene Arten des Datenschutzes. Volume 3 mit dem Titel „Supportive Analyses and References“ beschreibt potenzielle Schwachstellen aus verschiedenen Bereichen des Smart Grids.

3.3.7 NERC CIP

Das NERC ist eine Non-Profit-Organisation und ist für die nordamerikanischen Stromnetze zuständig. Die Abkürzung CIP in NERC CIP steht dabei für „Critical Infrastructure Protection“ und bietet standardisierte Handlungsempfehlungen in zehn Teilen (CIP-002 bis CIP-011) für die Zuverlässigkeit des amerikanischen Stromversorgungssystems aktuell in der fünften Revision. Es werden beispielsweise Hinweise für das Training von Personal oder für das Wartungs- und Änderungsmanagement gegeben[33].

3.3.8 ENISA: Appropriate security measures for smart grids[34]

ENISA steht für “European Network and Information Security Agency” (deutsch: Europäische Agentur für Netz und Informationssicherheit) und wurde von der Europäische Union gegründet, um Netz- und Informationssicherheit in der EU zu etablieren und zu verbessern. Diese Agentur hilft den EU-Mitgliedern in Sicherheitsfragen und unterstützt diese, indem Vorgaben und Empfehlungen in Bezug auf Netz- und Informationssicherheit durch die ENISA entwickelt werden. Ein Dokument mit dem Titel „Appropriate security measures for smart grids – Guidelines to assess the sophistication of security measures implementation“ wurde zu Sicherheitsmaßnahmen für das Smart Grid herausgegeben. Dabei vergleicht und bezieht sich die ENISA auf Sicherheitsmaßnahmen bereits bestehender Informationssicherheitsstandards, die teilweise auch in diesem Dokument beschrieben werden, und identifiziert Sicherheitsmaßnahmen für zehn Domänen. Die hier untersuchten Sicherheitsstandards sind die folgenden: NISTIR 7628, ISO/IEC 27002, (ISO/IEC DIS 27036-2), (ISO/IEC 27011), NERC CIP, IEC 62443, IEC 62351,

[33] Eine genauere Erläuterung beziehungsweise eine Zusammenfassung der Version 5 dieser Standards ist unter http://www.velaw.com/uploadedfiles/vesite/resources/summarycipversion5standards2014.pdf
zu finden. Die jeweilige aktuelle Version der einzelnen Standards ist auf der Homepage des NERC unter http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx abgelegt.

[34] Das Dokument kann unter https://www.enisa.europa.eu/publications/appropriate-security-measures-for-smart-grids/at_download/fullReport abgerufen werden.

ISO/IEC TR 27019, BDEW Whitepaper. Weiterhin werden unterschiedliche Reifegrade (sophistication level) von 1 bis 3 für jede Sicherheitsmaßnahme der zehn Domänen anhand unterschiedlicher Fortschrittsgrade der Sicherheitsrealisierung festgelegt. Dieses Dokument kann somit dafür genutzt werden, Reifegrade für die umgesetzte Informationssicherheit zu bestimmen und anschließend zu identifizieren, welche Maßnahmen ergriffen werden müssen, um die umgesetzte Informationssicherheit zu optimieren.

3.3.9 BSI TR-03109[35]

Die Technische Richtlinie (TR) BSI TR-03109 des BSI definiert die Anforderungen an die Funktionalität, Interoperabilität und Sicherheit, die die Einzelkomponenten in einem Smart Metering System erfüllen müssen, sowie die Anforderungen zur Prüfung dieser Eigenschaften. Sie besteht aus den Teilen TR-03109-1 bis TR-03109-6 sowie Testspezifikationen und Anlagen.

3.3.9.1 BSI TR-03109-1

Teil 1 der Technischen Richtlinie TR-03109 beinhaltet die funktionalen Anforderungen, die ein Smart-Meter-Gateway (SMGW) mindestens erfüllen muss. Das Dokument ist in die drei Themenbereiche Local Meteorological Network (LMN), Home Area Network (HAN) und Wide Area Network (WAN) untergliedert und definiert für diese Bereiche detaillierte technische Vorgaben. Darüber hinaus werden interne, logische Abläufe (bspw. die Tarifierung anhand von Regelwerken, Zusammenspiel zwischen Gateway und Sicherheitsmodul) weiter ausgeführt.

3.3.9.2 BSI TR-03109-2

In Teil 2 der Technischen Richtlinie TR-03109 werden die Anforderungen an die Funktionalität und Interoperabilität des Sicherheitsmoduls für das SMGW spezifiziert. Sie enthält neben einer detaillierten Beschreibung des Lebenszyklus-Modells von Sicherheitsmodul bzw. SMGW insbesondere die Spezifikation des File- und Objektsystems, der Zugriffsregeln und des Kommandosets des Sicherheitsmoduls. In einem Anhang zu dieser Technischen Richtlinie [TR-03109-2A] werden weitere Anwendungsfälle (Use Cases) mit einer Beschreibung der Nutzung des Sicherheitsmoduls durch das SMGW aufgeführt.

3.3.9.3 BSI TR-03109-3

Das Dokument enthält den Verweis, dass Vorgaben für die verbindlich einzusetzenden kryptographischen Verfahren und Primitive sowie die zu verwendenden Schlüssellängen in der jeweils aktuellen Fassung der BSI TR-03116, Teil 3 „Kryptographische Vorgaben für Projekte der Bundesregierung – Intelligente Messsysteme“ zu finden sind.

3.3.9.4 BSI TR-03109-4

[35] Informationen zur BSI TR-03109 stellt das BSI bereit unter https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03109/TR-03109_node.html
Informationen des BSI zum Schutzprofil des Smart Meter Gateways sowie zu der dazugehörigen Technischen Richtlinie TR-03109-1 können unter https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/SmartMeter/SmartMeterGateway/Schutzprofil_Gateway/schutzprofil_smartmetergateway_node.html abgerufen werden.

In der TR-03109-4 wird die Architektur der Smart Metering - Public Key Infrastruktur (SM-PKI) spezifiziert, mit der die Authentizität der bei der Kommunikation eingesetzten öffentlichen Schlüssel der Kommunikationspartner auf WAN-Ebene sichergestellt wird. Technisch wird der Authentizitätsnachweis der Schlüssel über digitale Zertifikate aus der SM-PKI realisiert.

Die TR enthält auch die Mindestanforderungen an die Interoperabilität und die Sicherheit der SM-PKI, die in der Zertifizierungsrichtlinie (Certificate Policy, CP) für die SM-PKI berücksichtigt werden müssen. Es werden für die einzusetzenden Zertifikate und Sperrlisten Profile vorgegeben. Ferner werden Protokolle für die Beantragung und Zustellung von Zertifikaten und ein Verzeichnisdienst zur Veröffentlichung der ausgestellten Zertifikate spezifiziert.

3.3.9.5 BSI TR-03109-5

Die „Technische Richtlinie Kommunikationsadapter“ befindet sich aktuell noch in Vorbereitung.

3.3.9.6 BSI TR-03109-6

Der Teil 6 der TR-03109 stellt normative Mindestanforderungen an die Informationssicherheit eines SMGW Admin. Diese Mindestanforderungen sind jeweils durch ein Informationssicherheitsmanagementsystem (ISMS) des SMGW Administrators zu behandeln und konkret auszugestalten. Die Prüfung der Ausgestaltung ist in einem Auditierungsschema geregelt.

Es werden zunächst die Aufgaben und Anwendungsfälle des SMGW Admin beschrieben. Diese leiten sich im Wesentlichen aus dem Gesetz über den Messstellenbetrieb und die Datenkommunikation in intelligenten Energienetzen (Messstellenbetriebsgesetz – MsbG) – Entwurf und BSI TR-03109-1 ab und werden in übersichtlicher Form zusammengefasst.

Das zentrale Kapitel 4 definiert die Sicherheitsanforderungen an den Betrieb des SMGW Admins im Sinne der Informationssicherheit. Dazu wird zunächst auf Schutzziele und zu berücksichtigende Bedrohungen eingegangen. Mindestvorgaben („Mindest-Maßnahmen“) zur Informationssicherheit werden für folgende Bereiche gestellt:

- Dokumentation von Prozessabläufen und Verantwortlichkeiten
- Sensibilisierung der Mitarbeiter
- Inferenzprävention
- Rollen- und Rechtekonzept
- Regelungen zur Vorhaltezeit und Aufbewahrungsdauer von Daten
- SMGW Admin Software und Frontend SMGW Admin Software
- Regelungen für Wartungs- und Reparaturarbeiten
- Entwicklung und Umsetzung eines Anbindungskonzeptes
- Einsatz Zeitserver mit gesetzlicher Zeit
- Netzsegmentierung und -trennung
- Integritätsschutz von IT-Systemen und IT-Komponenten
- Dienstsegmentierung
- Einsatz eines oder mehrerer Protokollierungsserver
- Penetrationstest
- Reaktion auf Verletzung der Sicherheitsvorgaben
- Aufrechterhaltung der Informationssicherheit

- Regelungen für den Einsatz von Fremdpersonal
- Schlüsselmanagement
- SMGW Firmware Update
- Notfallkonzept

Bei der Umsetzung der Anforderungen sind zwei Alternativen möglich: Zum einen die Vorgehensweise und Zertifizierung nach ISO 27001 auf Basis von IT-Grundschutz oder zum anderen die Vorgehensweise nach ISO 27001. Unabhängig von der gewählten Vorgehensweise sind in jedem Fall die Mindestanforderungen zu berücksichtigen und im Rahmen der jeweiligen Sicherheitskonzeption zu betrachten.

Abschließend werden in dem Dokument Rahmenbedingungen für die Auditierung und Zertifizierung aufgezeigt, mit denen die konzipierten Maßnahmen nachweislich geprüft und zertifiziert werden können.

3.3.10 BSI TR-03116-3

Die BSI TR-03109-3 verweist auf diesen Teil 3 der BSI TR-03116 mit dem Titel „Kryptographische Vorgaben für Projekte der Bundesregierung – Intelligente Messsysteme“ (BSI TR-03116-3). In ihm werden die Sicherheitsanforderungen für den Einsatz kryptographischer Verfahren in die Infrastruktur intelligenter Messsysteme im Energiesektor beschrieben. Im Einzelnen werden Anforderungen in folgenden Bereichen formuliert:

- Kryptografische Verfahren und Parameter
- TLS-Kommunikation im Weitverkehrsnetz (WAN)
- TLS-Kommunikation im Home Area Network (HAN)
- TLS-Kommunikation im lokalen metrologischen Netz (Local Metrological Network, LMN)
- Kommunikation im LMN auf Basis symmetrischer Kryptographie
- Inhaltsdatenverschlüsselung und -signatur
- PACE-Protokolle (Password Authenticated Connection Establishment) und Secure Messaging zur sicheren Kommunikation über einen verschlüsselten, authentisierten Kanal zwischen den Smart Meter Gateway und Sicherheitsmodul
- Zertifizierung von Smart Meter Gateways und Sicherheitsmodule nach den Common Criteria

3.3.11 BSI TR-03145

Die Technische Richtlinie BSI TR-03145 „Secure Certification Authority Operation“ wurde vom Bundesamt für Sicherheit in der Informationstechnik (BSI) herausgegeben. Sie formuliert Anforderungen an eine Certification Authority (CA) in einer Public-Key-Infrastruktur (PKI). Die Anforderungen („requirements“ in der englischsprachigen TR) leiten sich aus Funktionalitäten der CA und darauf wirkende Bedrohungen her. Die Anforderungen müssen durch entsprechende Maßnahmen umgesetzt werden. Sie sind als eine Ergänzung zu einem ebenfalls geforderten Informationssicherheitsmanagementsystem (ISMS) nach der internationalen Norm ISO/IEC 27001 oder nach ISO 27001 auf Basis IT-Grundschutz zu verstehen.

Die Umsetzung der Richtlinie kann als „sektorspezifische Zertifizierung“ zusammen mit der Etablierung des ISMS durch ein Zertifikat des BSI nachgewiesen werden. Das Zertifikat für den ISMS-Anteil kann auch auf Basis ISO 27001 von einer anderen dafür autorisierten Zertifizierungsstelle ausgestellt werden.

Die BSI TR-03145 ist klar strukturiert. Für die einzelnen Prozesse, Aufgaben und Funktionen einer CA sind zunächst die Ziele aufgeführt, gefolgt von Bedrohungen und Sicherheitsanforderungen sowie einer Gegenüberstellung und Begründung, wie den Bedrohungen durch Umsetzung der Anforderungen wirksam begegnet wird. Nach diesem Schema werden folgende Bereiche behandelt:

- Privater Schlüssel der CA
- Verbreitung der Geschäfts- und Nutzungsbedingungen und Regeln
- Identifizierung und Registrierung
- Verwaltung der Teilnehmerschlüssel
- Zertifikaterzeugung
- Verbreitung vertrauenswürdiger Zertifikate (public keys)
- Widerruf und Suspendierung von Zertifikaten und Suspendierung von Teilnehmern
- Zertifikatserneuerung, Rekeying und update

Darüber hinaus werden für folgende Bereiche generelle Sicherheitsanforderungen gestellt:

- ISMS
- Zertifikats-Policy und Zertifikats-Practice Statement
- Notfallmanagement und Behandlung von Sicherheitsvorfällen
- Prozessorganisation einschließlich nicht-digitaler Prozesse
- Kryptographische Maßnahmen
- Gesicherter Umgang und Speicherung von Schlüsseln
- Management von Rollen
- Vertrauenswürdiges Personal
- Gehärtete IT-Systeme und Netze mit Unterstützung von Logging und Monitoring
- Archivierung und Nachverfolgung
- Sichere Pflege und Verwaltung des Widerruf-Status
- Physische und umgebungsbezogene Sicherheit
- Verfügbarkeit von Diensten
- Sichere Beendigung einer CA
- Anforderungen an Unterauftragnehmer

3.3.12 Common Criteria (ISO/IEC 15408)

Die Common Criteria for Information Technology Security Evaluation (Common Criteria, CC; deutsch: Allgemeine Kriterien für die Bewertung der Sicherheit von Informationstechnologie) sind ein internationaler Standard zur Prüfung und Bewertung der Sicherheitseigenschaften von IT-Produkten.

Die Version 3.1 wurde 2006 im internationalen Common Criteria Anerkennungsabkommen verabschiedet und gemäß BSI-Zertifizierungsverordnung im Bundesanzeiger vom 23.02.2007

offiziell bekannt gegeben. Diese Version der CC liegt ebenfalls als internationaler Standard ISO/IEC 15408 vor. Ebenso verabschiedet wurde die gemeinsame Evaluationsmethodologie (Common Methodology for Information Security Evaluation CEM) Version 3.1 welche eine abgestimmte Methodik für die Evaluierung auf Grundlage der CC festlegt und auch als internationaler Standard ISO/IEC 18045 vorliegt.

Die CC umfassen drei Teile:

- Teil 1: Hier werden „Einführung und allgemeines Modell / Introduction and General Model“ die Grundlagen der IT-Sicherheitsevaluation und der allgemeine Geltungsbereich der CC erläutert. In den Anhängen werden Schutzprofile (Protection Profile) und Sicherheitsvorgaben (Security Target) für den zu prüfenden Evaluationsgegenstand (EVG) beschrieben.
- Teil 2: „Funktionale Sicherheitsanforderungen / Functional Requirements“ enthält Funktionalitätsanforderungen in Form eines Kataloges, welcher Empfehlungen (d.h. keine zwingenden Vorgaben) für die Beschreibung der Funktionalität eines Evaluationsgegenstandes macht. Die Zusammenhänge von Bedrohungen, Sicherheitszielen und funktionalen Anforderungen sind im Anhang erläutert.
- Teil 3: Hier werden „Anforderungen an die Vertrauenswürdigkeit / Assurance Requirements“ die Anforderungen an die Vertrauenswürdigkeit dargestellt.

Grundgedanke der CC ist die Unterscheidung zwischen der **Funktionalität** (Funktionsumfang) eines Systems und der **Vertrauenswürdigkeit** (Qualität).
Funktionale Sicherheitsanforderungen werden in Klassen zusammengefasst. Beispiele für wichtige Klassen sind:

- FAU Security Audit (Sicherheitsprotokollierung)
- FCO Communication (Kommunikation)
- FCS Cryptographic Support (Kryptographische Unterstützung)
- FDP User Data Protection (Schutz der Benutzerdaten)
- FIA Identification and Authentication (Identifikation und Authentisierung)
- FMT Security Management (Sicherheitsmanagement)
- FPR Privacy (Privatheit)
- FPT Protection of the TSF (Schutz der Sicherheitsfunktionen)
- FRU Ressource Utilisation (Betriebsmittelnutzung)
- FTA Target of Evaluation Access (Schnittstelle)
- FTP Trusted Path/Channels (Vertrauenswürdiger Pfad/Kanal)

Für die **Vertrauenswürdigkeit** sind sieben Abstufungen vorgesehen (Evaluation Assurance Level, EAL1-7). Sie spiegeln die Korrektheit der Implementierung des betrachteten Systems bzw. die Prüftiefe mit der dies nachgewiesen wurde wieder. Es sind:

- EAL1: funktionell getestet
- EAL2: strukturell getestet
- EAL3: methodisch getestet und überprüft
- EAL4: methodisch entwickelt, getestet und durchgesehen
- EAL5: semiformal entworfen und getestet
- EAL6: semiformal verifizierter Entwurf und getestet

- EAL7: formal verifizierter Entwurf und getestet

Anforderungen an die Funktionalität sowie an die Vertrauenswürdigkeit werden in **Schutzprofilen** zusammengefasst und decken eine bestimmte Menge von Sicherheitszielen vollständig ab. Es werden generische Anforderungen an eine Produktkategorie festgeschrieben, welche zunächst implementierungsunabhängig sind, und durch die daraus ableitbaren Sicherheitsvorgaben auf einen konkreten Evaluationsgegenstand (EVG) zugeschnitten werden können.

Beispiele für Schutzprofile des BSI sind:

- BSI-CC-PP-0073-2014 beschreibt die Anforderungen an ein Gateway, welches die zentrale Kommunikationseinheit für ein intelligentes Messsystem darstellt. Das Gateway stellt zentrale Funktionen zum sicheren Abruf, Speicherung, Aufbereitung und Versendung von Messdaten von einem oder mehreren Mandanten bereit.
- BSI-CC-PP-0077-V2-2015 beschreibt die Anforderungen an ein Sicherheitsmodul, das für den Einsatz in einem Smart-Meter-Gateway vorgesehen ist. Das Sicherheitsmodul stellt zentrale kryptografische Funktionen zur Verfügung, sowie das sichere Speichern kryptografischer Schlüssel und weiterer Daten, die für das Gateway relevant sind.

3.3.13 IEEE 1686-2007

Der Standard IEEE 1686-2007 mit dem Titel "IEEE Standard for Substation Intelligent Electronic Devices (IEDs) Cyber Security Capabilities" (deutsch: IEEE Standard für die Cybersicherheit von IEDs (Intelligente Elektronische Geräte) in Ortsnetzstationen) beschreibt Cybersicherheitsfunktionen für IEDs in Ortsnetzstationen. Der Standard unterstützt das US-Programm zum Schutz kritischer Infrastrukturen (CIP Critical Infrastructure Protection) und adressiert Sicherheitsaspekte von IEDs beim Zugriff, beim Betrieb, bei der Konfiguration, bei der Änderung von Firmware und beim Datenabruf. Verschlüsselung wird in diesem Standard nicht behandelt. Die Cybersicherheitsfunktionen werden in die folgenden Bereiche unterteilt und beschrieben:

- **Elektronische Zugriffskontrolle:** behandelt Sicherheitsfunktionen für den Zugriff jeder Art auf das IED, z.B. Vorgaben für Passwörter.
- **Protokollierung:** beschreibt wie und was innerhalb eine IEDs protokolliert werden soll, es werden z.B. 12 verschiedene Events festgelegt, die gespeichert werden sollen.
- **Überwachung und Kontrolle:** zusätzlich zur Protokollierung soll eine Überwachung von sicherheitsbezogene Aktivitäten vorhanden sein, es wird z.B. festgelegt in welchen Fällen ein Alarm erfolgen soll.
- **Konfigurationssoftware:** beschreibt Sicherheitsaspekte in Bezug auf die Konfigurationssoftware, wie z. B. dass der Zugriff auf die Konfigurationssoftware Login/Passwort-geschützt sein soll.
- **Zugriff auf die Kommunikationsports:** alle Ports bis auf den Diagnoseport sollen aktivier- und deaktivierbar sein.
- **Qualitätssicherung der Firmware:** die Qualitätssicherung der Firmware sollte gemäß IEEE Std C37-231.3 erfolgen.

3.3.14 IEEE Std C37.240-2014

Der Standard IEEE Std C37.240-2014 mit dem Titel "Cybersecurity Requirements for Substation Automation, Protection, and Control Systems" (deutsch: Cybersicherheitsanforderungen für Automation in Ortsnetzstationen, Schutz- und Leitsysteme) beschreibt technische Anforderungen für Cybersecurity für Ortsnetzstationen und dazugehörige Komponenten. In dem Standard wird versucht ein Gleichgewicht zu finden zwischen der technischen Ausführbarkeit und der finanziellen Machbarkeit. Die übergeordneten Schutzziele, die in diesem Standard behandelt werden, sind:

- Zugriffs- und Zugangskontrolle,
- Nutzungskontrolle,
- Datenintegrität und -vertraulichkeit,
- Datenflussbeschränkungen,
- Zeitnahe Reaktion auf ein Ereignis und
- Netzwerkverfügbarkeit.

Zusätzlich werden physische Sicherheit und gespeicherte Daten (Data-at-rest) als Schutzziel benannt.
Detaillierter werden dann die Anforderungen für Cybersecurity beschrieben. Zunächst wird auf die Methodik aus dem NISTIR 7628 hingewiesen, aus dem nach einem Mapping des eigenen Sicherheitsprogramms auf die Schnittstellenkategorien des NISTIR 7628 die Highlevel Anforderungen anhand des NISTIR 7628 auf Basis der Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit identifiziert werden können. Weiterhin werden die Sicherheitsanforderungen für folgende Kategorien beschrieben, wobei teilweise auf weitere IEEE-Standards verwiesen wird (IEEE 1615, 802.11, 802.15, 1686, 1711):

- **Systemkomponenten für Kommunikation:** macht Vorgaben verschiedene Systemkomponenten, die in Ortsnetzstationen für die Kommunikation verwendet werden, wie z.B. Router Switches o.ä. Weiterhin werden für die Komponenten dann z.B. Verschlüsselungsvorgaben, Vorgaben für die Authentifizierung oder auch für Firewalls, VPNs usw. gemacht.
- **Funktionale Anforderungen:** beschreibt funktionale Anforderungen für die Netzwerke, wie z.B. Kommunikationspfade, Einwahl per Remote aber auch Verschlüsselungsvorgaben.
- **Benutzerauthentifikation und -autorisation:** macht Vorgaben zur Nutzer Authentifizierung und Autorisierung, z. B. dass Multi-Faktor-Authentifizierung verwendet werden soll.
- **Schutz für Übertragungsdaten (Data-in-motion):** beschreibt den Schutz von Übertragungsdaten, z.B., dass Daten, die zwischen verschiedenen Sicherheitszonen ausgetauscht werden verschlüsselt werden müssen.
- **Konfigurationsmanagement:** macht Vorgaben zum zentralen Konfigurationsmanagement, z.B. welche Konfigurationen an der zentralen Stelle abgespeichert sein müssen.
- **Audits von Sicherheitsereignissen sowie Analyse und Reaktion von/auf Sicherheitsvorfälle:** beschreibt was anhand eines Sicherheitsvorfalls protokolliert werden soll, wie z.B. wo der Ursprung des Angriffs ist und welche Geräte betroffen sind.

- **Sicherheitstestfälle:** beschreibt Vorgaben, wie das Testen der Cybersicherheit erfolgen soll, z.B. wie oft und wer die Tests ausführen soll.

3.3.15 Ergebnisse und Fazit

Die folgende Tabelle 6 gibt einen Überblick über die in diesem Abschnitt 3.3 beschriebenen Normen, Standards und Richtlinien. Die Kategorien in den Tabellenspalten sind dabei angelehnt an die „Smart Energy Grid – Coordination Group“ von CEN-CENELEC-ETSI in ihrem „Cyber Security and Privacy“-Bericht.

Standard	Sprache		Ursprüngliche Domäne			Art der Vorgaben			Adressat		
	deutsch	englisch	Informationssysteme	Energieversorgung	Industrielle Automatisierung	Richtlinien	Anforderungen	Umsetzung	Betreiber	Systemintegrator	Entwickler
ISO/IEC 27001/02	x	x	x				x		x		
ISO/IEC TR 27019				x			x	x	x		
BSI IT Grundschutz	x		x					x		x	
BDEW Whitepaper	x	x		x			x		x	x	x
IEC 62351		x		x		x		x	x	x	x
IEC 62443		x			x		x	x	x	x	x
NISTIR 7628		x		x			x			x	x
NERC CIP		x		x			x	x	x		
ENISA „Smart Grid“		x		x		x			x	x	x
BSI TR-03109	x			x				x	x		x
BSI TR-03116-3	x			x				x			x
Common Criteria		x	x				x				x
BSI TR-03145		x	x					x			x
IEEE 1686-2007	x		x	x	x		x		x	x	x
IEEE Std. C37.240-2014	x		x	x	x		x		x	x	x

Tabelle 6: Übersichtstabelle Normen, Standards und Richtlinien

Die folgende Tabelle 7 ordnet die hier beschriebenen Normen, Standards und Richtlinien den einzelnen Arbeitspaketen (APs) aus enera zu. Dabei ist jeder AP-Nummer ein Kurztitel zur besseren Verständlichkeit angehängt. Diese Zuordnung zu den APs erfolgte im Rahmen von AS 12.2.1 und soll durch die Schnittstellenverantwortlichen für Informationssicherheit in den APs überprüft werden. Ein „x“ pro Zelle bedeutet dabei, dass das entsprechende Gesetz eine Relevanz für das AP aufweist.

AP-Nummer – Kurztitel	ISO/IEC 2700x	BSI Grundschutz	BDEW Whitepaper	IEC 62351	IEC 62443	NISTIR 7628	NERC CIP	ENISA	TR-03109	BSI TR-03116	Common Criteria	TR-03145
AP1 – Digitale Konnektivität	x	x	x			x		x	x	x	x	x
AP2 – SDSP	x	x	x			x		x				
AP3 – SG-Operator	x	x	x	x		x	x	x	x	x	x	
AP4 – Rollout Netzbetriebsmittel	x	x	x	x		x	x	x				
AP5 – Flexibilisierung	x	x	x			x		x				
AP6 – Technische Entwicklung regionaler Produkte	x	x	x			x		x				
AP7 – Marktintegration regionaler Produkte	x	x										
AP8 – Energierecht												
AP9 – Neue Geschäftsmodelle	x	x										
AP10 – enera Qualifizierungscenter												
AP11 – Bürgerbeteiligung	x	x										
AP12 – Architektur und Security	x	x	x	x	x	x	x	x	x	x	x	x
AP13 – Nationaler/Internat. Transfer	x			x			x	x				
AP14 – Projektmanagement												

Tabelle 7: Relevanz der Normen, Standards und Richtlinien für die einzelnen APs in enera

3.4 Informationssicherheit in der Software Entwicklung

Grundsätzlich orientiert sich der Bedarf an Sicherheit einer Software-Lösung an den Anforderungen der Domäne, in denen die Software zum Einsatz kommt bzw. kommen soll. Allgemeingültige und übergreifende Anforderungen an die Sicherheit von Software sind daher nicht vorhanden. Unabhängig von expliziten Anforderungen besteht beim Einsatz von Software jedoch bei allen Anwendern der grundlegende Bedarf, dass diese sicher ist und wie erwartet zur Verfügung steht. Außerdem muss es sich um wirtschaftlich angemessene Sicherheitslösungen handeln.

Bei der Entwicklung von Software-Lösungen sind daher die Anforderungen an die Sicherheit(sfunktionen) der Software vorab zu klären (Anforderungsmanagement). Diese Anforderungen sind anschließend im Rahmen der Softwareentwicklung zu berücksichtigen sowie umzusetzen. Vor Abschluss der Entwicklungstätigkeiten sind die implementierten Sicherheitsfunktionen innerhalb des Testmanagements zu überprüfen. Hierbei sollten zusätzliche Testfälle definiert werden, welche nicht nur die Funktionsfähigkeit sicherstellen, sondern auch die Robustheit (Verhalten im Fehlerfall). Alle Tätigkeiten werden in der Regel über die Verfahren zur Softwareentwicklung koordiniert, welche nachfolgend kurz erläutert werden.

3.4.1 Klassische Verfahren Softwareentwicklung

3.4.1.1 V-Modell

Das V-Modell wird als ein generalisierter Rohling deklariert, welcher auf ein konkretes Projekt angepasst werden kann. Anders als bei sonstigen klassischen Modellen werden im V-Modell **Aktivitäten** und **Ergebnisse** definiert. Auf eine zeitlich strikte Abfolge wird dabei verzichtet. Darüber hinaus fehlen die typischen Abnahmen, welche Phasenenden definieren. Dennoch ist es möglich, die Aktivitäten des V-Modells zum Beispiel auf ein Wasserfallmodell abzubilden. Die Grundelemente des V-Modells bilden folgende Komponenten:

- Aktivitäten: Tätigkeiten im Software-Entwicklungsprozess
- Ergebnisse: Artefakte der Aktivitäten

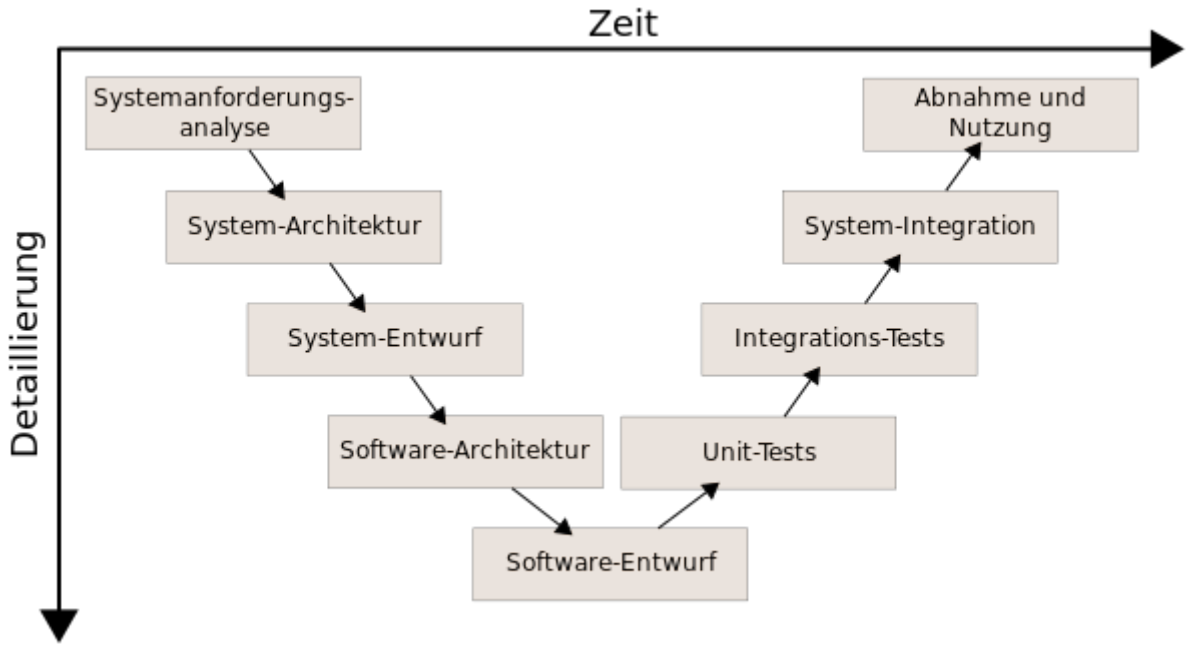


Abbildung 7: Schema des V-Modells (Quelle: Michael Pätzold, S. Seyfert)

Das V-Modell wird immer in folgende Sub-Modelle untergliedert. Nicht benötigte Aktivitäten und Ergebnisse werden nach Bedarf herausgenommen, dies ist das sogenannte „Tayloring“.

- Software-Erstellung
- Qualitätssicherung
- Konfigurationsmanagement und
- Projektmanagement

3.4.1.2 Wasserfallmodell

Das Wasserfallmodell setzt sich aus den folgenden Schritten zusammen:

- Aufstellen der Anforderungen
- Systemanalyse
- Systementwurf
- Implementierung
- Test und Integration

- Abnahme

Jeder dieser Schritte wird im Wasserfallmodell als genau eine Phase abgebildet. Daher handelt es sich bei einem Wasserfallmodell um ein Phasenmodell. Jede Phase hat eine definierte Aufgabenstellung, die zu einem definierten Phasenergebnis führen soll.

Das Ergebnis einer Phase stellt die Eingabe und den Start der nächsten Phase dar. Wenn die vorherige Phase mit einer Qualitätsprüfung freigegeben und abgeschlossen wurde, kann die nächste Phase begonnen werden. Bei entdeckten Fehlern oder Änderungswünschen während der Qualitätsprüfung, kann die nächste Phase nicht angestoßen werden. Erst die Freigabe – aufgrund einer ausreichenden Qualität – durch einen Verantwortlichen, führt zum Sprung in die nächste Phase. Werden an den Phasengrenzen der sequentiellen Entwicklungsschritte Qualitätsprüfungen durchgeführt, so kann das Wasserfallmodell als Baseline Management-Modell bezeichnet werden.

Die folgende schematische Darstellung[36] zeigt die Abfolge der Phasen im Wasserfallmodell:

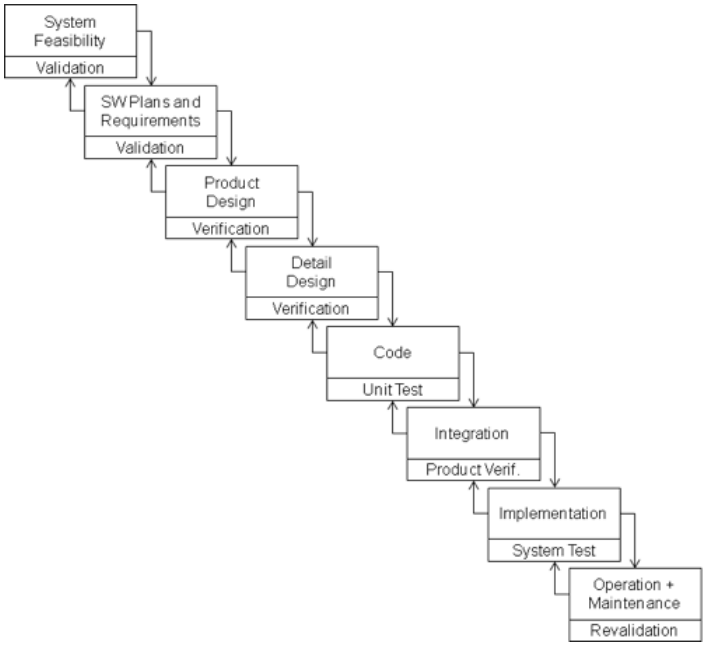


Abbildung 8: Schema des Wasserfallmodells

3.4.2 Agile Verfahren in der Softwareentwicklung

Für Vorgehensweisen in der klassischen Softwareentwicklung wird grundsätzlich der Begriff **Vorgehensmodell** verwendet. In der agilen Softwareentwicklung ist die Verwendung des Begriffs Vorgehensmodell schwierig, da Schwerpunkte vielmehr auf Werte und Praktiken statt auf organisatorische Rahmen gelegt werden. Daher wird in diesem Zusammenhang der Begriff **Methodik** angewendet. Allen Methoden der agilen Softwareentwicklung liegt das Agile Manifest zugrunde. Die jeweiligen Vorgehensweisen und Konzepte basieren auf den dort erwähnten Werten.

[36] Quelle: https://www.enzyklopaedie-der-wirtschaftsinformatik.de/lexikon/is-management/Systementwicklung/Vorgehensmodell/Wasserfallmodell/index.html

Wesentlich für agile Softwareentwicklungen sind möglichst **häufige Rückkopplungsprozesse** und zyklische (iterative) Vorgehensweisen auf allen Ebenen. Mit Ebenen sind hier die Teams, das Management und die Programmierung gemeint. Das neu zu entwickelnde System wird bei der agilen Softwareentwicklung nicht im Vorfeld detailliert geplant und dann in einem einzigen Lauf entwickelt. Bei der Entwicklung wechseln kurze Planungs- und Entwicklungsphasen miteinander ab. Ein Plan für eine erste Version wird dann ausgearbeitet, wenn eine erste Vision, also die Ziele für das System, festgelegt und gewichtet worden sind. Notwendige Anpassungen bezüglich der Entwicklungsgeschwindigkeit, der organisatorischen Rahmenbedingungen und der möglichen Probleme, werden erst nach diesem Schritt durchgeführt. Eine Basisversion mit den wichtigsten Features soll möglichst schnell entwickelt werden, um diese gemeinsam mit dem Kunden zu bewerten, erforderliche Anpassungen vorzunehmen und nachfolgende Versionen besser optimieren zu können.

Um diesen Anforderungen gerecht zu werden, soll der Kunde mit dem Management und den Entwicklern eng zusammenarbeiten und in Standup-Meetings gerade fertiggestellte und zeitnah anfallende Arbeiten kommunizieren. Die von Kunde und Management vorgegebenen Geschäftsziele sollen mit jeder neuen Software in Anforderungen überführt werden, denen das neue System entsprechen soll.

Im Rahmen der agilen Softwareentwicklung bestehen folgende agile Methoden:

- **Scrum**
  Scrum richtet sich eher in Richtung Management aus. Dabei werden grundsätzlich Intervalle von 30 Tagen angelegt, in denen eine bestimmte Anzahl von Anforderungen abgearbeitet werden sollen. Diese Anforderungen wurden im Vorhinein priorisiert (Backlog). Zusätzlich findet jeden Tag ein 15-minütiges Scrum Meeting statt, welches die hauptsächliche Koordination der Beteiligten regelt.
- **Xtreme Programming (XP)**
  XP ist eine der beliebtesten agilen Methoden, die aus den Erfahrungen bei der Entwicklung eines Informationssystems bei Daimler Chrysler entstanden ist und als sehr prinzipientreu gilt. Alle in XP definierten Methoden sollten gemäß Lehrbuch angewendet werden. Praktiken wie User Stories, Pair Programming, Simple Design, Test First und Continuous Integration sind umzusetzen.
- **Adaptive Software Development (ASD)**
  ASD entstand als Reaktion auf Turbolenzen der Industrie und mit dem Wunsch nach schneller Umsetzung von fachlichen Anforderungen. ASD bietet eine philosophische Basis und einen praxisorientierten Ansatz. Dabei spielten iterative Entwicklungsprozesse, Feature-Based Planning und eine Fokussierung auf Kundenanforderungen entscheidende Rollen.
- **Feature-Driven Development (FDD)**
  Ein sehr leichtgewichtiger, architekturbasierter Prozess, welcher zu Beginn eine Gesamtübersicht zur Architektur und Features auflistet. Anschließend werden Methoden wie Design-By-Feature und Build-By-Feature angewendet. Zentrale Rollen sind hierbei der Chef Architekt und der Chef Entwickler. UML und andere Objektorientierte Design Methoden spielen eine zentrale Rolle.

3.4.3 Security-by-Design Prinzipien und Security Patterns

Auch wenn es keine allgemeingültigen Anforderungen an Software-Lösungen gibt, so existieren Grundsätze bzw. Prinzipien, welche bei Berücksichtigung insbesondere kritische Sicherheitslücken bei Systemen vermeiden können. Dabei sind diese **Prinzipien** als Ziele zu verstehen, welche im Kontext des jeweiligen Entwicklungsvorhabens auf Anwendbarkeit geprüft sowie entsprechend umgesetzt werden können.

- **Minimierung der Angriffsfläche**
  Jede Funktion, die einer Anwendung hinzugefügt wird, fügt der Gesamtanwendung ein gewisses Risiko hinzu. Ziel der sicheren Entwicklung ist es, das Gesamtrisiko durch eine Verringerung der Angriffsfläche zu reduzieren. Zum Beispiel ist in einer Web-Anwendung eine Online-Hilfe mit einer Suchfunktion vorhanden. Die Suchfunktion kann anfällig für SQL-Injection-Angriffe sein. Wenn die Hilfefunktion auf autorisierte Benutzer beschränkt ist, wird die Angriffswahrscheinlichkeit reduziert.
- **Nutzung sicherer Standardwerte**
  Es gibt viele Möglichkeiten, um eine „out of the box“ Erfahrung für Benutzer zu liefern. Allerdings sollte die Erfahrung standardmäßig sicher sein und es dem Benutzer überlassen werden, die Sicherheit zu reduzieren, wenn dies zulässig ist. Beispielsweise sollten Kennwortgültigkeit und Komplexität standardmäßig aktiviert sein. Benutzer können diese beiden Funktionen ausschalten, um die Nutzung der Anwendung zu vereinfachen, dabei wird gleichzeitig das eigene Risiko erhöht.
- **Prinzip der geringsten Berechtigung**
  Das Prinzip der geringsten Berechtigung empfiehlt, dass Konten die geringste Berechtigung für die Ausführung ihrer Aktivitäten haben. Dies umfasst Benutzerrechte, Ressourcenberechtigungen wie CPU-Grenzwerte, Speicher-, Netzwerk- und Dateisystemberechtigungen. Zum Beispiel, wenn ein Proxy-Server nur Zugriff auf das Netzwerk, lesenden Zugriff auf eine Datenbanktabelle und die Möglichkeit in ein Protokoll zu schreiben erfordert, werden alle erforderlichen Berechtigungen in einer entsprechenden Rolle zusammengefasst. Unter keinen Umständen sollten dem Server Administratorrechte eingeräumt werden.
  Ein Konzept dieses Prinzip umzusetzen ist die rollenbasierte Zugriffskontrolle (engl. role based access control, RBAC). Dabei werden den Nutzern Rollen zugewiesen, so dass sie nur minimale Rechte und somit nur Zugriff haben, um ihre entsprechenden Aufgaben zu erfüllen. Ein Nutzer kann je nach Aufgabentätigkeit mehreren Rollen zugeordnet sein.
- **Prinzip „Defense in depth“**
  Das Prinzip „Defense in depth“ verfolgt, dass dort, wo eine Kontrolle sinnvoll ist, mehrere Kontrollen, die die Risiken in unterschiedlicher Weise vermeiden, besser sind. Denn verschachtelte und tief im System befindliche Kontrollen können außerordentlich schwierig ausgenutzt werden und sind somit unwahrscheinlich als Quellen für schwerwiegende Sicherheitslücken. Dies kann in Form von mehrstufigen Validierungen, zentralisierten Audit-Kontrollen und stetige Prüfung auf autorisierte Benutzer erfolgen.
- **Vollständige Zugriffskontrolle**

Jeder Objektzugriff muss hinsichtlich seiner Berechtigung geprüft werden. Der Hintergedanke ist hierbei, die Autorisierung nicht nur an einer Stelle durchzuführen und Auswirkungen von Fehlern in der Implementierung so einzuschränken. Beispielsweise sollte nach diesem Prinzip nicht nur der Zugriff auf bestimmte Objekte in der Präsentationsschicht, sondern (sofern möglich) auch auf Datenbankebene geprüft werden.

- **Sichere Fehlerbehandlung und Protokollierung**
  Anwendungen schlagen regelmäßig bei der Abarbeitung von Transaktionen fehl – aus unterschiedlichsten Gründen. Es ist daher stets auf eine sichere Fehlerbehandlung im Rahmen der Anwendung zu achten. Damit Angriffe auf Anwendungen (überhaupt) nachvollzogen werden können, ist es erforderlich, dass die in der Anwendung aufgetretenen Fehler in sicherheitsrelevanten Funktionen (etwa bei der Authentisierung) protokolliert werden.
- **Vertrau keinen IT-Services**
  Viele Organisationen nutzen die Verarbeitungskapazitäten von Dritten, die sehr wahrscheinlich andere Sicherheitsrichtlinien und -vorgaben haben als die Organisation selbst. Es ist unüblich, dass Vorgaben bei Externen von außen beeinflusst oder kontrolliert werden können. Daher ist ein implizites Vertrauen für extern betriebene Systeme nicht gerechtfertigt. Alle externen Systeme sollten in ähnlicher Weise behandelt werden. Zum Beispiel sollten Daten, welche von einem externen System verarbeitet und zurückgespielt werden, vor der Weiterverarbeitung auf Plausibilität überprüft werden.
- **Minimale gemeinsame Ressourcen**
  Der Zugriff auf gemeinsam genutzte Ressourcen, wie beispielsweise globale Variablen, durch mehrere Benutzer oder Prozesse ist weitestgehend zu minimieren. Jede gemeinsam genutzte Ressource enthält mögliche unerwünschte Informationsflüsse. Auch kann dies dazu führen, dass ein Benutzer (oder Prozess) die Ressourcen eines anderen beeinflusst. Wenn möglich sollen gemeinsam genutzte Ressourcen daher sinnvoll separiert werden. Dies kann zum Beispiel durch den Einsatz lokaler Variablen bzw. Virtualisierung geschehen.
- **Trennung von Rollen**
  Ein Schlüssel zum Schutz vor Betrug ist die Trennung von Rollen. Zum Beispiel muss, wenn eine Person (z.B. ein Angestellter) eine Zahlung anweist, eine weitere Person mit einer anderen Rolle (z.B. sein Vorgesetzter) diese Zahlung bestätigen. Bestimmte Rollen haben ein anderes Vertrauenslevel als normale Benutzer. Insbesondere sind Administratoren anders zu handhaben als normale Benutzer. Im Allgemeinen sollten Administratoren nicht auch Benutzer der Anwendung sein. Zum Beispiel sollte ein Administrator in der Lage sein, das System ein- oder auszuschalten oder die Kennwortrichtlinie festzulegen, nicht aber sich am Webportal als hochprivilegierter Benutzer anzumelden, um zum Beispiel Waren im Namen anderer Benutzer zu kaufen.
- **„Keep it simple“**
  Angriffsfläche und Einfachheit gehen Hand in Hand. Neue Vorgehensweisen bevorzugen teilweise übermäßig komplexe Ansätze, die sonst mit relativ einfachen Methoden gelöst werden könnte. Entwickler sollten die Verwendung von doppelten negativen Prüfungen und komplexen Architekturen vermeiden, wenn ein alternativer / klassischer Ansatz schneller und einfacher wäre.

- **Sicherheitsprobleme richtig beheben**
  Sobald ein Sicherheitsproblem identifiziert wurde, ist es wichtig, einen Test für dieses zu entwickeln und die Ursache des Problems zu verstehen. Wenn Design-Muster verwendet werden, ist es wahrscheinlich, dass das Problem in der Anwendung weit verbreitet ist. Die Entwicklung der richtigen Korrektur ohne Einführung von neuen Schwachstellen ist daher von wesentlicher Bedeutung, um das System vollständig abzusichern.

Weiterhin können **Security Patterns** bei der Berücksichtigung von Sicherheitslösungen in der Softwareentwicklung verwendet werden. Entwurfsmuster bzw. „Software Patterns“ liefern eine abstrahierte Lösung für ein Problem, das in einem spezifischen Kontext auftritt. Sie bieten also auch Lösungen, die unabhängig von der Programmiersprache sind. Neben Entwurfsmustern[37] für eine Architektur gibt es spezielle Entwurfsmuster für den Bereich der Informationssicherheit (Security Patterns). Diese Entwurfsmuster abstrahieren Lösungen für typische Sicherheitsprobleme in bestimmten Kontexten.

Die Dokumentation von Patterns für die Informationssicherheit unterscheidet sich kaum von typischen Software Patterns. Neben einer allgemeinen Beschreibung enthält ein Entwurfsmuster typischerweise den vorgesehenen Kontext und eine abstrakte Problem- sowie Lösungsbeschreibung. Weiterhin sind Informationen wie Implementierungshinweise, Beispiele, bekannte Einsatzgebiete und mögliche Seiteneffekte sinnvolle Ergänzungen.

Entwurfsmuster für Informationssicherheit lassen sich in verschiedene Bereiche einordnen wie Entwurfsmuster für das Risikomanagement, zur Zugriffskontrolle, für Firewall-Architekturen und Entwurfsmuster für sichere Webanwendungen. Nach Schumacher et al.[38] erfolgt die Unterteilung der Security Pattern Landschaft in folgende Kategorien:

- Enterprise Security and Risk Management Patterns
- Identification & Authentication (I&A) Patterns
- Access Control Model Patterns
- System Access Control Architecture Patterns
- Operating System Access Control Patterns
- Accounting Patterns
- Firewall Architecture Patterns
- Secure Internet Applications Patterns
- Cryptographic Key Management Patterns
- Related Security Pattern Repositories Patterns

3.4.4 Best Practices für Software(entwicklung)

Zur Erhöhung der Sicherheit von Software ist es ebenfalls sinnvoll, auf Erfahrungen und erfolgreichen Lösungswegen (Best Practices) von Dritten aufzubauen. Oft lassen sich von den Lösungen Ansätze für die eigenen Entwicklungstätigkeiten ableiten. Hierfür ist es sinnvoll, die in der jeweiligen Technologie führenden Fachgremien bzgl. vorhandener Best Practices zu

[37] Siehe z.B. “Design Patterns: Elements of Reusable Object-Oriented Software” von Gamma, Helm, Johnson, Vlissides.
[38] Siehe “Security Patterns - Integrating Security and Systems Engineering” von Schumacher, Fernandez-Buglioni, Hybertson, Buschmann, Sommerlad

kontaktieren. Ebenfalls bieten viele Hersteller von Basiskomponenten (wie z. B. einem Betriebssystem oder einer Datenbanklösung) Hinweise und Empfehlungen zur sicheren Verwendung der jeweiligen Technologie.

Ergänzend gibt es allgemeine Übersichten zu Sicherheitsproblemen, welche häufig zu Sicherheitslücken geführt haben. Hier sei als Beispiel auf das Open Web Application Security Project (OWASP) verwiesen, welches regelmäßig die aktuellen „Top-Bedrohungen" im Kontext von Web-Applikationen39 sowie mobilen Applikationen40 zur Verfügung stellt.

Insgesamt gilt es wiederkehrende Muster von Schwachstellen zu vermeiden[41]: An erster Stelle sind dies **Designfehler**, z.B. die mehrfache Haltung von Benutzerdaten, die besonders geschützt sein sollten, in verschiedenen Datenbanken. Bei Designfehlern besteht meist die Notwendigkeit eines Redesigns. Im Vergleich dazu können Codingfehler meist mit lokalem Patch behoben werden. Es besteht außerdem häufig das Problem **unsicher mit Ein- und Ausgaben umzugehen**, beispielsweise SQL-Injection oder Cross-site Scripting (siehe auch OWASP Top 10). Maßnahmen hierbei sind die Input-Validierung, d.h. die Eingaben genau darauf prüfen, ob sie enthalten, was erwartet wird, also Whitelisting statt Blacklisting zu betreiben. Außerdem sollte Output Sanitisierung verwendet werden, d.h. Ausgaben genau darauf prüfen, ob sie enthalten, was erwartet wird und nur in dem gewünschten Typ (z.B. ein Bild). Auch wenn ein hoher Aufwand nötig ist diese Schwachstelle auszunutzen, ist es wichtig nicht **unsicher im Umgang mit dem Speicher** zu sein und somit z.B. Buffer Overflows zu vermeiden. Man kann dies umgehen, indem man sichere Funktionen und Sprachen verwendet, also keine Programmiersprachen, die Speichermanipulation erlauben bzw. nur Funktionen verwenden, die den Speicherbereich kontrollieren. Weiterhin ist der **unsichere Umgang mit Wettlaufsituationen (race conditions)** ein wiederkehrendes Muster, beispielsweise der gleichzeitige Zugriff auf gemeinsame Informationen. Dies lässt sich verhindern, indem atomare Funktionen verwendet werden. Auch der **unsichere Umgang mit Berechtigungen und Ressourcen** spielt häufig eine Rolle bei den Schwachstellen einer Implementierung. Z.B. der nicht autorisierte Zugriff auf Informationen sollte vermieden werden. Hier sollten minimale Rechte gesetzt werden, z.B. Zugriffe auf die Sichtbarkeit von Ressourcen sollten eingeschränkt sein. Diese Muster von Schwachstellen werden u.a. durch die OWASP Top 10 oder auch die „24 Sins of Software Security"[42] abgedeckt.

3.4.5 Anforderungen an Softwareentwicklung gemäß BSI

Zur Orientierung, welche Aktivitäten im Rahmen der Softwareentwicklung zu berücksichtigen sind, um eine möglichst hohe Sicherheit der Software zu erreichen, hat das BSI die Bausteine

[39] https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project
[40] https://www.owasp.org/index.php/OWASP_Mobile_Security_Project#Top_Ten_Mobile_Risks
[41] Siehe Buch "Basiswissen Sichere Software – Aus- und Weiterbildung zum ISSECO Certified Professional for Secure Software Engineering" von Sachar Paulus.
[42] Siehe Buch "24 Deadly Sins of Software Security – Programming Flaws and How to Fix Them", Michael Howard, David LeBlanc, John Viega, McGrawHill, 2010.

„CON.5 Entwicklung und Einsatz von Individualsoftware“[43] und „CON.8 Software-Entwicklung“[44] im BSI IT-Grundschutzkompendium (siehe oben in Kapitel 3.3.2.6) zur Verfügung gestellt. Die Bausteine beschäftigen sich mit allen relevanten Aspekten, die von Institutionen bei der Entwicklung von Software zu beachten sind.

Hierzu werden Vorbereitung, Durchführung und Inbetriebnahme seitens der Institution betrachtet und die relevanten Gefährdungen und Anforderungen dargestellt. Dabei ist es von wesentlicher Bedeutung, dass die Informationssicherheit über den gesamten Software-Entwicklungsprozess hinweg berücksichtigt wird, da nur auf diese Weise die Informationssicherheit der zu entwickelnden Software-Lösung im Rahmen des Entwicklungsprojektes selbst gewährleistet werden kann.

Weitere Bausteine wie „OPS.1.1.3 Patch- und Änderungsmanagement“ und „OPS.1.1.6 Software-Tests und Freigaben“ enthalten ergänzende Anforderungen.

In der folgenden Aufzählung werden die Anforderungen (A+Nummer) im Baustein „CON.8 Software-Entwicklung“ kurz in Stichworten umrissen:

- **A1 Definition von Rollen und Verantwortlichkeiten**
  Benennung eines Gesamtverantwortlichen, eines Sicherheitsverantwortlichen, und weitere.
- **A2 Auswahl eines Vorgehensmodells**
  Auswahl eines geeigneten Vorgehensmodells, Festlegung Ablaufplan, Dokumentation der Sicherheitsanforderungen, Schulung des Personals zum Vorgehensmodell
- **A3 Auswahl einer Entwicklungsumgebung**
  Auswahl der Entwicklungsumgebung anhand einer vorher festgelegten Liste der erforderlichen und optionalen Auswahlkriterien.
- **A4 Einhaltung einer sicheren Vorgehensweise**
  Einhaltung des Vorgehensmodells, Prüfung von Quellcode und externen Komponenten.
- **A5 Sicheres Systemdesign**
  Validierung aller Daten bei Eingabe und Weiterverarbeitung, Konfiguration von Standardeinstellungen, Schutz kritischer Informationen, minimale Benutzerprivilegien, Dokumentation und Überprüfung des Systemdesigns.
- **A6 Verwendung von Bibliotheken aus vertrauenswürdigen Quellen**
  Integrität und vertrauenswürdige Quellen eingesetzter Bibliotheken
- **A7 Anwendung von Testverfahren**
  Durchführung angemessener, umfassender Tests und Code Reviews. Überprüfung der Systemvoraussetzungen auf ausreichende Dimensionierung.
- **A8 Bereitstellung von Patches, Updates und Änderungen**
  Zeitnahes Einspielen von sicherheitskritischen Patches und Updates, digitale Signaturen.

[43] Siehe auf der Homepage des BSI: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/CON/CON_5_Entwicklung_und_Einsatz_von_Individualsoftware.html
[44] Siehe auf der Homepage des BSI: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/CON/CON_8_Software-Entwicklung.html

- **A9 Berücksichtigung von Compliance-Anforderungen**
  Alle Compliance-Anforderungen, institutionsweite Sicherheitsrichtlinien, rechtliche Anforderungen und spezifische Sicherheitsanforderungen.
- **A10 Versionsverwaltung des Quellcodes**
  Einsatz einer geeigneten Versionsverwaltung mit entsprechenden Regelungen.
- **A11 Erstellung einer Richtlinie für die Software-Entwicklung**
  Verbindliche Vorgaben u. a. zu Namenskonventionen, zulässigen und unzulässigen Elementen.
- **A12 Ausführliche Dokumentation**
  Projekt-, Funktions-, Schnittstellendokumentation, Administratoren- und Anwender-Hilfen.
- **A13 Beschaffung von Werkzeugen**
  Beschaffung nach standardisierten und dokumentierten Vorgehensweisen
- **A14 Schulung des Projektteams zur Informationssicherheit**
  Allgemeine und spezifische Schulungen
- **A15 Sicherer Einsatz der Test- und Entwicklungsumgebungen**
  Getrennter Betrieb der Entwicklungs- und Testumgebungen vom Produktivbetrieb, Testdaten, gesicherte Verbindungen bei verteilten Arbeitsplätzen, kontrollierter Zugriff.
- **A16 Geeignete Steuerung der Software-Entwicklung**
  Projektmanagement entsprechend Vorgehensmodell, Qualifikation des Personals, Abdeckung des gesamten Software-Lebenszyklus. Risikomanagement und Festlegung von Qualitätszielen.

Bei erhöhtem Schutzbedarf sind ergänzend diese weiteren Anforderungen umzusetzen:

- **A17 Auswahl vertrauenswürdiger Entwicklungswerkzeuge**
- **A18 Regelmäßige Sicherheitsaudits für die Entwicklungsumgebung**
- **A19 Regelmäßige Integritätsprüfung der Entwicklungsumgebung**

3.4.6 Ergebnisse und Fazit

Dieser Abschnitt hat verschiedene Verfahren, Prinzipen und Best Practices vorgestellt und somit Möglichkeiten für die Berücksichtigung von Sicherheit in der Softwareentwicklung aufgezeigt. Die Anwendung der einzelnen Vorschläge unterliegt in enera den einzelnen Entwicklungsvorhaben und Anwendungsfällen, so dass hier keine allgemeine tabellarische Kategorisierung pro Arbeitspaket (AP), wie in den Abschnitten 3.2 und 3.3, erfolgen kann.

3.5 Zertifizierungen

In diesem Abschnitt werden Zertifizierung in Bezug auf Informationssicherheit, die für das Projekt enera relevant sind, kurz beschrieben. Abschnitt 3.5.1 befasst sich mit der Zertifizierung eines ISMS nach der internationalen Norm DIN ISO/IEC 27001. Abschnitt 3.5.2 erläutert die Zertifizierung von ISO 27001 nach IT-Grundschutz. In 3.5.3 werden Zertifizierungen im Rahmen des IT-Sicherheitskatalogs erörtert. Abschnitt 3.5.4 beschreibt die Zertifizierung des Smart Meter Gateway Administrators nach BSI TR 03109-6 und Abschnitt 3.5.5 erläutert die

Zertifizierung eine Certification Authority (CA) für eine Public-Key-Infrastruktur, um das Sicherheitsniveau aller Teilnehmer nachzuweisen.

3.5.1 DIN ISO/IEC 27001

Die Auditierung und Zertifizierung zum Standard DIN ISO/IEC 27001 bezieht sich auf ein Informationssicherheitsmanagementsystem (Information Security Management System - ISMS), welches prozessorientiert alle für einen ausgewiesenen Geltungsbereich relevanten Werte zur Informationssicherheit umfasst. Das ISMS und die Zertifizierung dienen zum Schutz der Unternehmenswerte und Geschäftsprozesse, zum Management von Informationssicherheits-Risiken und zum Sicherheitsnachweis der Organisation gegenüber dem Gesetzgeber, Kunden, Partnern, Versicherungen und Lieferanten.

3.5.1.1 Relevanz

Die Norm mit zugehöriger Zertifizierung hat international einen großen Stellenwert. Viele Konzerne fordern von Zulieferern und Partnern ein Zertifikat zum Nachweis des Sicherheitsniveaus. Die Zertifizierung des ISMS nach DIN ISO/IEC 27001 ist unverzichtbar zur Erfüllung der Anforderungen des IT-Sicherheitskataloges und – alternativ zu ISO 27001 auf Basis IT-Grundschutz – zwingend erforderlich für die Konformität zur TR 03109-6 und zur TR 03145.

3.5.1.2 Auditierungs- und Zertifizierungsschema

Die Auditierung erfolgt in 2 Stufen („stage 1“ und „stage 2“). Wichtige Elemente die geprüft werden sind u.a. Verantwortlichkeiten, Prozesse, Dokumentationen, die Risikoanalyse, das statement of applicability, interne Audits und Managementberichte. Ebenso ist der Anhang A normativ. D.h. die dort vorgegebenen Maßnahmenziele und Maßnahmen sind grundsätzlich umzusetzen, wobei allerdings plausible Ausschlüsse erlaubt sind und bei der Umsetzung relativ große Freiheiten bestehen. DIN ISO/IEC 27002 ist nicht Gegenstand der Zertifizierung, sie bietet Unterstützung, indem sie die Controls der 27001 detaillierter beschreibt, sie ist aber nicht zwingend. Ein Zertifikat gilt (ebenso wie das für ISO 27001 auf Basis IT-Grundschutz) drei Jahre und muss jährlich durch ein Überwachungsaudit bestätigt werden.

3.5.1.3 Zertifizierungsstelle und Auditoren

Die Zertifizierung erfolgt durch eine akkreditierte Zertifizierungsstelle. Bei der Deutschen Akkreditierungsstelle (DAkkS) sind derzeit mehr als 25 Zertifizierungsstellen gelistet45, das BSI gehört nicht dazu.

Die Auditoren werden von den Zertifizierungsstellen berufen. Sie müssen eine entsprechende Ausbildung und Erfahrung nachweisen.

3.5.2 ISO 27001 auf Basis IT-Grundschutz

ISO 27001-Zertifizierungen auf der Basis von IT-Grundschutz sind seit 2006 durch das BSI möglich. Sie integrieren die Norm DIN ISO/IEC 27001 mit der Grundschutzvorgehensweise

[45] Siehe auch http://www.dakks.de/content/akkreditierte-stellen-dakks.

und den Grundschutzkatalogen. Daneben gibt es noch die beiden Vorstufen „Auditor-Testat IT-Grundschutz Einstiegsstufe" und „Auditor-Testat IT-Grundschutz Aufbaustufe". Diese stellen einfachere Varianten mit geringeren Anforderungen dar und können im Regelfall durch einen zertifizierten Auditor selbständig, ohne Zertifizierungsstelle erbracht werden.

3.5.2.1 Relevanz

Der IT-Grundschutz hat in Deutschland und teilweise der DACH-Region einen sehr hohen Stellenwert. Hinsichtlich der zugehörigen Zertifizierung sind viele Organisationen allerdings zurückhaltender, wenngleich in den letzten Jahren eine deutliche Steigerung spürbar war. Die Zertifizierung des ISMS nach ISO 27001 auf Basis IT-Grundschutz – oder alternativ DIN ISO/IEC 27002 – ist zwingend erforderlich für die Konformität zur TR 03109-6 und zur TR 03145.

3.5.2.2 Auditierungs- und Zertifizierungsschema

Vom BSI werden ein Auditierungsschema („Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz Auditierungsschema, Version 1.0“) und ein Zertifizierungsschema („Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz Zertifizierungsschema, Version 1.2“) vorgegeben, in welchen die Abläufe genau und verbindlich festgelegt sind.46

Eine Zusammenfassung des Auditierungs- und Zertifizierungsprozesses ist in Abbildung 9 dargestellt (Quelle: BSI).

[46] Siehe auch https://www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/Managementsystemzertifizierung/Zertifizierung27001/Zertifizierungsschema/schema_node.html;jsessionid=B8D8408880C1DFFB0872A297263557B9.1_cid341

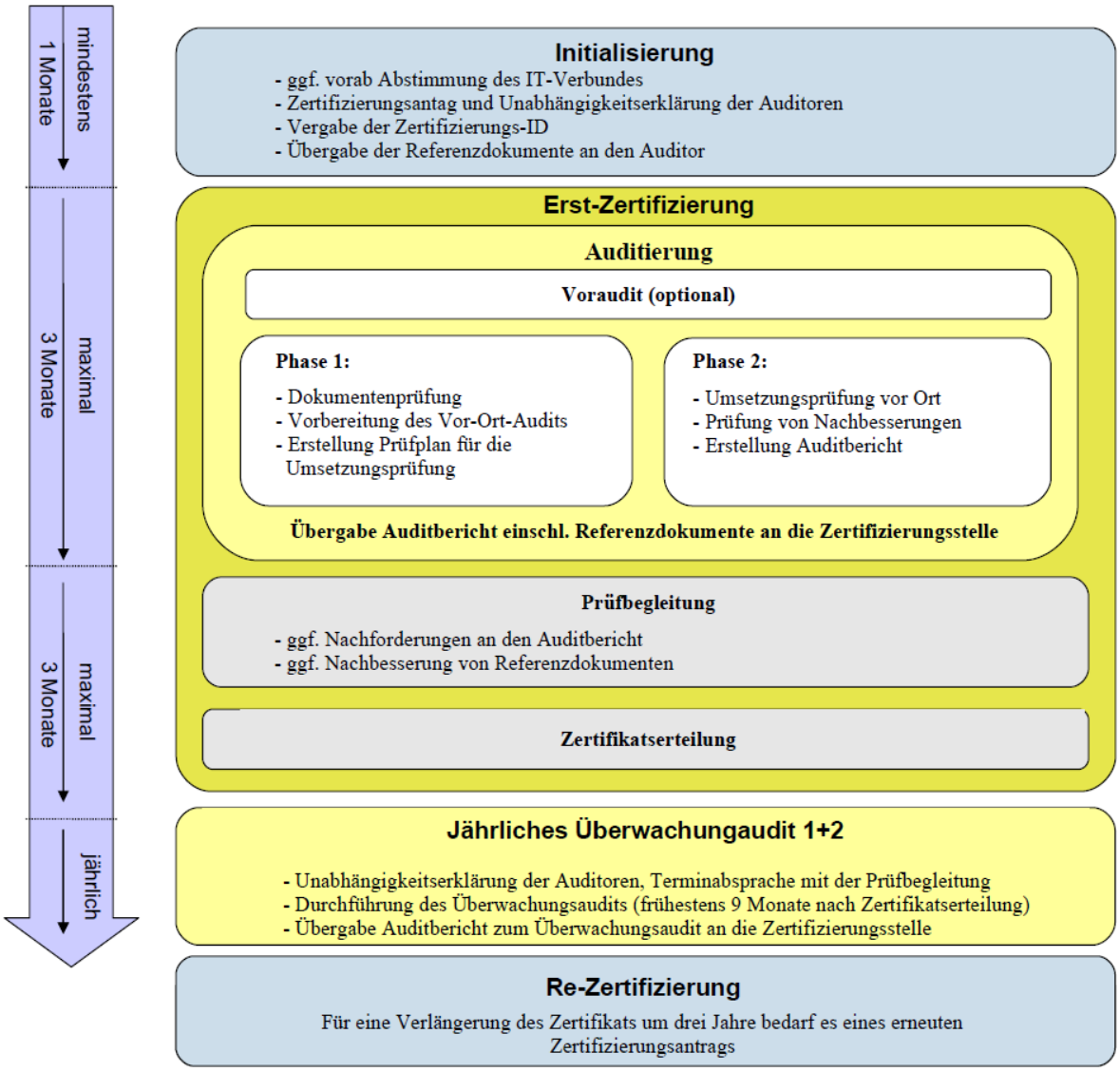


Abbildung 9: Übersicht Auditierung und Zertifizierung ISO 27001 auf Basis IT-Grundschutz (Quelle: BSI)

3.5.2.3 Zertifizierungsstelle und Auditoren

Zertifizierungsstelle ist das BSI. Zertifizierungsanträge und Unabhängigkeitserklärungen müssen beim BSI eingereicht werden. Mit der Vergabe der Zertifizierungsnummer beginnt das Audit. Der vom Auditor erstellte Auditbericht wird vom BSI genau geprüft, bevor dieses, ggf. nach der Erfüllung von Nachforderungen, das Zertifikat vergibt.

Die Auditoren müssen relevante Erfahrungen und Kenntnisse nachweisen und eine Schulung mit Prüfung beim BSI absolvieren. Sie bekommen dann für drei Jahre eine Personenzertifizierung (ebenfalls durch das BSI), welche nach Ablauf durch Nachweis ausreichender Auditaktivitäten verlängert werden kann. Die Auditoren schließen mit dem BSI einen Vertrag, stehen aber in keinem Arbeitsverhältnis zum BSI.

3.5.3 IT-Sicherheitskatalog

Der IT-Sicherheitskatalog enthält Anforderungen zur Gewährleistung eines angemessenen Schutzes gegen Bedrohungen für Telekommunikations- und elektronische Datenverarbeitungssysteme, die für einen sicheren Netzbetrieb notwendig sind. Er wurde von der Bundesnetzagentur (BNetzA) auf Grundlage von § 11 Abs. 1a des Energiewirtschaftsgesetzes (EnWG) veröffentlicht. Netzbetreiber werden verpflichtet, ihr Informationssicherheits-Managementsystem (ISMS) gemäß DIN ISO/IEC 27001 zertifizieren zu lassen, wobei neben DIN ISO/IEC 27002 zusätzlich Maßnahmen zur DIN ISO/IEC TR 27019 umzusetzen sind (Erweiterung der DIN ISO/IEC 27002 um spezifische Aspekte im Bereich der Prozesssteuerung der Energieversorgung).

3.5.3.1 Relevanz

Die Verantwortung für die Umsetzung der Vorgaben des IT-Sicherheitskatalogs haben die bei der BNetzA gelisteten Betreibern eines Strom- oder Gasnetzes. Dies gilt unabhängig davon, ob ein Netzbetreiber ein Strom- oder Gasnetz als Eigentümer oder im Rahmen eines Pachtmodells betreibt. Ausnahmen von der Umsetzungspflicht, etwa in Abhängigkeit von der Größe eines Netzbetreibers, bestehen nicht.

Die erfolgreiche Umsetzung der Anforderungen muss mit einer Zertifizierung nachgewiesen werden. Diese muss in Form einer Kopie des Zertifikats der Bundesnetzagentur vorliegen. Zur Frist für die Vorlage des Nachweises siehe Kapitel 3.2.5.

3.5.3.2 Auditierungs- und Zertifizierungsschema

Die Abläufe für Auditierung und Zertifizierung entsprechen im Wesentlichen denen einer reinen ISO 27001 Zertifizierung. Besonderes Augenmerk wird auf die Abgrenzung des Geltungsbereichs gelegt. Dieser muss zumindest alle TK- und EDV-Systeme des Netzbetreibers umfassen, welche direkt Teil der Netzsteuerung sind, d. h. unmittelbar Einfluss nehmen auf die Netzfahrweise. Daneben sind auch TK- und EDV-Systeme im Netz betroffen, die selbst zwar nicht direkt Teil der Netzsteuerung sind, deren Ausfall jedoch die Sicherheit des Netzbetriebs gefährden könnte.

Insbesondere zur Prüfung der Abgrenzung des Geltungsbereichs und der Risikoanalyse muss das Audit-Team einen Fachexperten hinzuziehen. Der Fachexperte soll das Auditteam bei der Einschätzung, ob alle für den Netzbetrieb notwendigen Systeme, Komponenten und Anwendungen im Scope erfasst sind und die Risikoeinschätzung korrekt durchgeführt worden ist, beraten. Er muss neben einem ingenieur- oder naturwissenschaftlichen (Fach-)Hochschulstudium mindestens drei Jahre einschlägige Berufserfahrung in der leitungsgebundenen Energieversorgung nachweisen. Die Unterstützung durch einen Fachexperten kann entfallen, sofern ein Mitglied des Audit-Teams bereits mindestens fünf Mal zusammen mit einem Fachexperten auditiert hat.

3.5.3.3 Zertifizierungsstelle und Auditoren

Die akkreditierten Stellen zur Zertifizierung des IT-Sicherheitskatalogs sind marktbekannte Stellen zur Zertifizierung von Managementsystemen. Sie können auf der Internetseite der DAkkS abgerufen werden.

Stand 20170612 sind cert GmbH, TÜV NORD CERT GmbH, TÜV Rheinland Cert GmbH, TÜV SÜD Management Service GmbH Zertifizierungsstelle und Kiwa International Cert GmbH gelistet.
Auditoren, die Netzbetreiber auditieren möchten, müssen die Anforderungen des Konformitätsbewertungsprogramms zur Akkreditierung von Zertifizierungsstellen für den IT-Sicherheitskatalog gemäß § 11 Absatz 1a Energiewirtschaftsgesetz auf der Grundlage der ISO/IEC 27006 erfüllen. Sie müssen bei einer akkreditierten Zertifizierungsstelle lizenziert sein und eine von der Bundesnetzagentur anerkannte Schulung zu den Grundlagen der leitungsgebundenen Energieversorgung mit Strom und Gas erfolgreich absolviert haben.

3.5.4 Smart Meter Gateway Administrator

Der SMGW Admin-Betrieb ist ein Bereich mit kritischen Anwendungen. Die Umsetzung der in Kapitel 4 der TR 03109-6 aufgeführten Mindestvorgaben bzgl. der zu betrachtenden Bedrohungen und der diesen entgegenwirkenden geeigneten und angemessenen Maßnahmen sind daher im Rahmen einer Auditierung zu prüfen und durch eine abschließende Zertifizierung des ISMS zu bestätigen.

3.5.4.1 Relevanz

Die Zertifizierung ist für den SMGW Admin-Betrieb zwingend erforderlich.

3.5.4.2 Auditierungs- und Zertifizierungsschema

Die Auditierung erfolgt in den zwei Phasen Dokumentenprüfung und Prüfung der Umsetzung der in der Dokumentation beschriebenen Prozesse und Maßnahmen.

Die für die Phase der Dokumentenprüfung vorzulegende Dokumentation besteht aus der individuellen Sicherheitskonzeption des zu prüfenden SMGW Admin und beinhaltet insbesondere die unter Kapitel 4.5.1 der TR 03109-6 geforderten Dokumentation der internen Prozessabläufe sowie IT-Sicherheitsrichtlinien, die Risikoanalyse und die Ergebnisse der IT-Penetrationstests. Weitergehende Dokumente kann der Auditor nach seinem Ermessen nachfordern.

Die vorgelegte Dokumentation ist vom Auditor dahingehend zu prüfen, ob sie die geforderten Inhalte nachvollziehbar und konsistent darstellt. Festgestellte Mängel sind vor der Prüfung der Umsetzung zu beheben und erneut durch den Auditor zu prüfen.

Im Rahmen der zweiten Audit-Phase muss der Auditor zwingend die Umsetzung der geforderten Sicherheitskonzeption prüfen.

Der Auditor hat dabei insbesondere zu prüfen, ob bei der Durchführung der Risikoanalyse die in dieser Technischen Richtlinie festgelegten Assets, Schutzziele und Bedrohungen beachtet und ausreichend behandelt bzw. bewertet wurden. Ebenso ist während des Audits zu verifizieren, ob die normativen Vorgaben zu den Maßnahmen beachtet und angemessen umgesetzt wurden.

3.5.4.3 Zertifizierungsstelle und Auditoren

Eine Zertifizierung/Konformitätsprüfung nach der TR 03109-6 erfolgt immer im Zusammenhang mit einer Zertifizierung nach ISO/IEC 27001 oder ISO 27001 auf Basis von IT-Grundschutz. Somit ist entweder zwingend das BSI oder eine bei der Deutschen Akkreditierungsstelle (DAkkS) gemäß ISO/IEC 27006 für ISMS akkreditierte Organisation als Zertifizierungsstelle involviert.

Auditoren müssen sich beim BSI qualifizieren. Es gelten die „Verfahrensbeschreibung zur Kompetenzfeststellung und Zertifizierung von Personen“ und das dazugehörige Dokument „Anforderungen an Antragsteller zur Zertifizierung als Auditor“ Diese sind in der jeweils aktuellen Version auf der Internetseite des BSI verfügbar.

3.5.5 Secure CA Operations

Nur eine sichere Certification Authority (CA) kann als Wurzel für eine Public Key Infrastruktur dienen, welche für die Sicherung von Vertraulichkeit Authentizität und Integrität von Informationen genutzt wird. Die BSI TR-03145 hat zum Ziel, CA zu unterstützen um ein angemessenes Sicherheitsniveau zu erreichen, indem organisatorische und technische Maßnahmen implementiert und Regeln für alle PKI-Teilnehmer aufgestellt werden. Die Zertifizierung dient dem Nachweis des Sicherheitsniveaus um auch das notwendige Vertrauen der anderen PKI-Teilnehmer zu erhalten.

3.5.5.1 Relevanz

Trust Center, die sich in der Smart Metering Public Key Infrastruktur (SM-PKI) als Smart Meter Certification Authority (CA) beteiligen möchten, müssen gemäß der Certificate Policy der Smart Metering-PKI eine Zertifizierung gemäß BSI TR-03145 „Secure CA Operation“ zusammen mit einer Zertifizierung ihres Informationssicherheitsmanagementsystems gemäß ISO/IEC 27001 oder ISO 27001 auf Basis IT-Grundschutz nachweisen.

3.5.5.2 Auditierungs- und Zertifizierungsschema

Es gibt seitens des BSI kein explizites Zertifizierungsschema. Ein Auditor soll das vom BSI herausgegebene Dokument „Secure CA operation, Part 2 Inspection specifications considering Trust Center (TC) instantiating as Certification Authority (CA) in Public-Key Infrastructure (PKI) with security level high'“ als Vorlage bzw. Checkliste nutzen. Für jede relevante der mehr als 200 Anforderungen muss mindestens ein Plausibilitätsnachweis erbracht (und für den Prüfbericht dokumentiert) werden, dass sie erfüllt ist.

3.5.5.3 Zertifizierungsstelle und Auditoren

Eine Zertifizierung/Konformitätsprüfung nach der TR 03145 erfolgt immer im Zusammenhang mit einer Zertifizierung nach ISO/IEC 27001 oder ISO 27001 auf Basis von IT-Grundschutz. Somit ist entweder zwingend das BSI oder eine bei der Deutschen Akkreditierungsstelle (DAkkS) gemäß ISO/IEC 27006 für ISMS akkreditierte Organisation als Zertifizierungsstelle involviert.

Auditoren müssen sich beim BSI qualifizieren. Es gelten die „Verfahrensbeschreibung zur Kompetenzfeststellung und Zertifizierung von Personen“ und das dazugehörige Dokument

„Anforderungen an Antragsteller zur Zertifizierung als Auditor“ Diese sind in der jeweils aktuellen Version auf der Internetseite des BSI verfügbar.

3.5.6 Ergebnisse und Fazit

Dieser Abschnitt erläuterte verschiedene Zertifizierungen in Bezug auf Informationssicherheit. Diese Zertifizierungen sind im Rahmen des Projekts enera relevant. In der folgenden Tabelle 8 wird eine Zuordnung der beschriebenen Zertifizierungen zu den APs vorgenommen. Dabei ist jeder AP-Nummer ein Kurztitel zur besseren Verständlichkeit angehängt. Diese Zuordnung zu den APs erfolgte im Rahmen von AS 12.2.1 und soll durch die Schnittstellenverantwortlichen für Informationssicherheit in den APs überprüft werden. Ein „x“ pro Zelle bedeutet dabei, dass das entsprechende Gesetz eine Relevanz für das AP aufweist.

AP-Nummer – Kurztitel	**DIN ISO/IEC 27001**	**ISO 27001 auf Basis IT-Grundschutz**	**IT-Sicherheitskatalog**	**Smart Meter Gateway Administrator**	**Secure CA Operations**
AP1 – Digitale Konnektivität	x	x	x	x	x
AP2 – SDSP	x	x	x		
AP3 – SG-Operator	x	x	x	x	
AP4 – Rollout Netzbetriebsmittel	x	x	x		
AP5 – Flexibilisierung	x	x	x		
AP6 – Technische Entwicklung regionaler Produkte	x	x	x		
AP7 – Marktintegration regionaler Produkte	x	x			
AP8 – Energierecht	x	x			
AP9 – Neue Geschäftsmodelle	x	x			
AP10 – enera Qualifizierungscenter	x	x			
AP11 – Bürgerbeteiligung	x	x			
AP12 – Architektur und Security	x	x	x	x	x
AP13 – Nationaler/Internat. Transfer	x				
AP14 – Projektmanagement					

Tabelle 8: Relevanz der Zertifizierungen für die einzelnen APs aus enera

4 Zusammenfassung und Ausblick

Ziel im AS 12.2.4 war es, die in dem Ergebnisbericht zu AS 12.2.1 bereits identifizierten Regularien, Compliance-Empfehlungen und Zertifizierungen im Bereich Informationssicherheit bis zum Projektende 2020 zu überwachen und die entsprechenden Übersichten und Umsetzungsempfehlungen bei Bedarf zu aktualisieren und zu erweitern bzw. zu ergänzen. Der Fokus lag auf den Regularien, Compliance-Empfehlungen und Zertifizierungen, die in den einzelnen APs zu berücksichtigen sind. Inhaltlich konnte der AS 12.2.4 also auf den bereits vorliegenden Ergebnissen des AS 12.2.1 aufsetzen. Alle dort getroffenen Zuordnungen und Empfehlungen erwiesen sich im weiteren Projektverlauf als tragfähig und gelten daher grundsätzlich weiterhin.

Die wesentlichste Änderung während der Projektlaufzeit betraf die Umstellung des BSI IT-Grundschutz (siehe Kapitel 3.3.2): Die BSI-Standards 200-1 „Managementsysteme für Informationssicherheit (ISMS)“, 200-2 „IT-Grundschutz-Methodik“ und 200-3 „Risikoanalyse auf der Basis von IT-Grundschutz“ lösten die jeweiligen Vorgänger-Standards ab, und das IT-Grundschutzkompendium tritt seit 2018 an die Stelle der IT-Grundschutzkataloge. Neben Änderungen im Zuschnitt der Bausteine und der Zuordnung von Sicherheitsanforderungen und –Maßnahmen wird hier auch der aktuelle Stand der Technik berücksichtigt. Bezogen auf die einzelnen enera-Arbeitspakete waren diese Änderungen in den ISMS der Konsortialpartner und in den eingesetzten Methoden und Werkzeugen zum IT-Grundschutz zu berücksichtigen, sie hatten jedoch keine wesentlichen inhaltlichen Auswirkungen.

Weitere Änderungen betrafen die Ausgestaltung einzelner Gesetze und Richtlinien, so z. B. die Umsetzung der EU-DSGVO im deutschen „Datenschutz-Anpassungs- und -Umsetzungsgesetz EU“, aber auch hier gab es keine kritischen Auswirkungen auf die Umsetzung in den Arbeitspaketen.

Noch bestehender Anpassungs- und Ergänzungsbedarf im Bereich Regularien, Compliance-Empfehlungen und Zertifizierungen wurde ebenfalls identifiziert, insbesondere das Erfordernis, die Ansätze zum Notfallmanagement im Bereich Energieversorgung zusammenzuführen und die Zertifizierungen zur Informationssicherheit für Energieversorger nach BSI IT-Grundschutz zu stärken, sowie der Bedarf nach Regelungen zu IT-Sicherheitskennzeichen und zur transparenten Lieferkette. Detaillierte Ausführungen hierzu befinden sich im Ergebnisdokument zum AS 12.2.22 „Gap-Analyse“.

Die weitere Konsolidierung des im AS 12.2.4 betrachteten Standes der Regularien, Compliance-Empfehlungen und Zertifizierungen im Bereich Informationssicherheit ist Aufgabe der bereits begonnenen Ergebnissynthese SINTEG im Themenfeld „Infrastruktur, Interoperabilität und Standardisierung“ des Synthesefeldes „Digitalisierung“, die voraussichtlich in 2022 abgeschlossen sein wird.

Literaturverzeichnis

[BSI 18]

Bundesamt für Sicherheit in der Informationstechnik (2018): Das BSI arbeitet für die IT-Sicherheit der Informationsgesellschaft. Online im Internet: https://www.bsi.bund.de/DE/Home/home_node.html

[BSI 20]
Bundesamt für Sicherheit in der Informationstechnik (2020): Glossar der Cyber-Sicherheit, Glossar und Begriffsdefinitionen. Online im Internet: https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Empfehlungen/cyberglossar/cyberglossar_node.html

[CONT 18]
Controlling-Portal (2018): Fachinfo, Risikomanagement. Online im Internet, URL: https://www.controllingportal.de/Fachinfo/Risikomanagement/Corporate-Governance.html.

[GABL 20]
Gabler Wirtschaftslexikon (2020): Definition. Online im Internet, URL: https://wirtschaftslexikon.gabler.de/definition/compliance-27721

Ergebnisdokument AS 12.2.13: Methoden und Verfahren zur Systementwicklung

Anpassungen des Use Case-Templates hinsichtlich Security-by-Design

Autoren:

Marie Clausen, Christine Rosinger (beide OFFIS), Rolf Apel (Siemens), Tobias Richter (PPC), Ulrike Henschel (IABG), Denis Uecker, Reinhard Schwarz (beide Fraunhofer IESE)

19.03.2021

Gefördert durch:

Bundesministerium für Wirtschaft und Energie

aufgrund eines Beschlusses des Deutschen Bundestages

Historie des Dokuments:

Version	Datum	Name	Änderungen	Dateiname
0.01	16.10.2019	Clausen	Erste Erstellung & Gliederung	20191016_AS12.2.13_Security-by-Design.docx
0.02	04.12.2019	Henschel	Ergänzungen in Kapitel 4	20191204_AS12.2.13_Security-by-Design_0_02.docx
0.03	10.12.2019	Henschel	Verbesserungen nach Input von OFFIS, Ergänzungen in Kapitel 4 und 5	20191210_AS12.2.13_Security-by-Design_0_03.docx
0.04	06.01.2020	Henschel	Verbesserungen und Ergänzungen nach Input von OFFIS	20200106_AS12.2.13_Security-by-Design_0_04.docx
0.05	19.02.2020	Henschel	Anpassungen, u. a. aus Input von OFFIS	20200219_AS12.2.13_Security-by-Design_0_05.docx
0.06	28.02.2020	Apel	Ergänzung aus Masterarbeit Lukas Engel	20200228_AS12.2.13_Security-by-Design_0_05.docx
0.07	13.03.2020	Clausen	Ergänzung zu Use Cases und Neustrukturierung Kapitel 3	20200313_AS12.2.13_Security-by-Design_0_07.docx
0.08	16.04.2020	Apel/ Clausen	Zusammenführung mit Ergänzungen Apel im Anhang, Überarbeitung Kapitel 4	20200416_AS12.2.13_Security-by-Design_0_08.docx
0.09	06.05.2020	Clausen	Weitere Ergänzungen	20200506_AS12.2.13_Security-by-Design_0_09.docx
auch 0.09	14.05.2020	div.	div. kleinere Korrekturen schon eingearbeitet	20200514_AS12.2.13_Security-by-Design_0_09_Komm UHeCRoUHe.docx
0.10	20.05.2020	Clausen	Ergänzung Anforderungskatalog & Beispiel Use Case, Kürzung Beispiel	20200520_AS12.2.13_Security-by-Design_0_10.docx
0.11	25.05.2020	Rosinger	Ergänzungen von FhG IESE eingearbeitet	20200525_AS12.2.13_Security-by-Design_0_11.docx
0.12	12.03.2021	Rosinger	Weitere Überarbeitungen und Prefinalisierung	20210312_AS12.2.13_Security-by-Design_0_12.docx
1.0	19.03.2021	Rosinger	Kommentare von Marie und Ulrike eingearbeitet und Dokument finalisiert.	20210319_AS12.2.13_Security-by-Design_1_0.docx

Inhalt

Abkürzungsverzeichnis 5
1 Allgemeine Einordnung und Gliederung 7
2 Grundlagen: Security im UC-Template 8
2.1 Security-by-Design 8
2.2 Use Cases bei enera 9
2.2.1 Beschreibung des Use Case-Templates 10
2.2.2 Vorgehen im Projekt 11
2.3 Use Cases als Grundlage für ein ISMS 12
2.4 Ziele der Anpassungen 14
3 Integration BSI IT-Grundschutz in UC-Template 16
3.1 Geschäftsprozesse und zugehörige Informationen 17
3.2 Anwendungen, IT-Systeme und Räume 19
3.3 Kommunikationsverbindungen 20
4 Ableitung von Empfehlungen aus enera Erfahrungen für die Anpassung des UC-Templates 22
4.1 Allgemeine Erfahrungen bei der Erfassung von Use Cases 22
4.2 Erfahrungen aus der Strukturanalyse und Inventarisierung 23
4.3 Erfahrungen aus der Schutzbedarfsfeststellung 24
4.4 Erfahrungen aus der Risikoanalyse 25
4.5 Ableitung von Empfehlungen 25
4.5.1 Empfehlungen zur Dokumentation 25
4.5.2 Empfehlungen zur Ergänzung von Informationen 26
4.5.3 Empfehlungen zur organisatorischen Bearbeitung 28
4.5.4 Zusammenfassung der Empfehlungen 28
5 Übergreifenden Listen und Katalogen 30
5.1 Relevante Asset-Typen 30
5.2 ENTSO-e Harmonized Electricity Role Model 31
5.3 Erstellung von Informationsobjektkatalogen 33
5.4 Beispiel für einen Informationsobjektekatalog 34
5.5 Beispiel für einen Anforderungskatalog 38
5.5.1 BSI Grundschutzkompendium 41
5.5.2 BDEW Whitepaper 41

6 Use Case-Template: Vorschläge zu Erweiterungen und verbesserter Nutzung 43
6.1 UC-Template Abschnitt 1 (“Description of the use case”) 43
6.2 UC-Template Abschnitt 2 (“Diagrams of use case”) 44
6.3 UC-Template Abschnitt 3 („Technical details“) 44
6.4 UC-Template Abschnitt 4 (“Step by step analysis of use case”) 45
6.5 UC-Template Abschnitt 5 („Information exchanged“) 46
6.6 UC-Template Abschnitt 6 (“Requirements (optional)”) 47
7 Zusammenfassung der Empfehlungen und Anpassungen 48
A.1 Anhang 1: Beispiel Use Case – Architekturdokumentation und Repository 55
A.2 Anhang 2: Beispiel Use Case – Datentechnische Betriebsabläufe in einem Virtuellen Kraftwerk 71

Abkürzungsverzeichnis

Abkürzung	Bedeutung
AP	Arbeitspaket
BDEW	Bundesverband der Energie- und Wasserwirtschaft e.V.
BMWi	Bundesministerium für Wirtschaft und Energie
BSI	Bundesamt für Sicherheit in der Informationstechnik
CEM	Customer Energy Management
CEN-CENELEC	Europäische Komitee für elektrotechnische Normung
CIM	Common Information Model
CLC	Abk. von CENELEC
CLS	Controllable Local System
DER	Dezentrale Energie Ressource
EMS	Energiemanagementsystem
ENTSO-E	European Network of Transmission System Operators for Electricity, Verband Europäischer Übertragungsnetzbetreiber
ESCO	Energy Service Company
HBES	Home and Building Electronic Systems
HL	High Level
HS	Hochspannung
IEC	International Electrotechnical Commission
ISMS	Informationssicherheitsmanagementsystem
ISO	International Organization for Standardization
IT	Informationstechnik
kV	Kilovolt
LFC	Low Frequency Current
MDM	Meter Data Management
MID	Measuring Instruments Device
mME	Moderne Messeinrichtung
M2M	Machine to machine
NET	Netze
NS	Niederspannung
PDCA	Plan-Do-Check-Act-Zyklus
SCADA	Supervisory Control and Data Acquisition
SGAM	Smart Grid Architecture Model

Abkürzung	Bedeutung
SINTEG	Schaufenster intelligente Energie - Digitale Agenda für die Energiewende
SMGW	Smart Meter Gateway
TAP	Teilarbeitspaket
UC	Use Case
UCMR	Use Case Management Repository
V	Volt

Ergebnisdokument AS 12.2.13

Anpassungen des Use Case-Templates hinsichtlich Security-by-Design

1 Allgemeine Einordnung und Gliederung

Enera ist eins der fünf durch das Bundesministeriums für Wirtschaft und Energie (BMWi) geförderten Projekte des Förderprogramms „Schaufenster intelligente Energie – Digitale Agenda für die Energiewende“ (SINTEG)[1]. Im Projekt werden Lösungen zu den drei Themenschwerpunkten Netz, Markt und Daten in der Modellregion im Nordwesten Niedersachsens entwickelt und erprobt. Das Arbeitspaket (AP) 12 innerhalb dieses Projekts beschäftigt sich mit der informationstechnischen Entwicklung der enera Gesamtarchitektur inklusive eines Informationssicherheitskonzepts.

Das Teilarbeitspaket (TAP) 12.2 befasst sich mit dem Informationssicherheitskonzept. Der dazugehörige Arbeitsschritt (AS) 12.2.13 „Methoden und Verfahren zur Systementwicklung“ befasst sich mit Use Cases (UC) als Methode zur Systementwicklung, die in TAP 12.1 angewandt wurde und auf der die weiteren Arbeiten in TAP 12.2 aufgesetzt haben. Innerhalb dieses Dokuments soll das UC-Template nach IEC 62559 in der Art angepasst werden, dass Informationssicherheitsaspekte bereits bei der Anwendungsfallerfassung mitberücksichtigt werden, also ein Security-by-Design-Vorgehen etabliert werden kann.

Dafür gliedert sich dieses Dokument nach dieser ersten Einordnung im Projekt im weiteren Verlauf wie folgt:

- Zunächst werden in *Kapitel 2* Grundlagen beschrieben, wie bspw. das Prinzip Security-by-Design oder das Use Case Template selbst, das anfangs in enera, auch ohne den Hintergrund ein Informationssicherheitsmanagementsystem (ISMS) zu erstellen, genutzt wurde.
- In *Kapitel 3* wird beschrieben, wie man den BSI IT-Grundschutz (BSI IT-GS) in das bestehende Use Case-Template (UC-Template) integrieren kann, ohne großartige Änderungen vorzunehmen.
- *Kapitel 4* beschreibt dann verschiedene Erfahrungen – mit der Erfassung von Use Cases und der Erstellung eines ISMS – und daraus abgeleitete Empfehlungen.
- Danach wird in *Kapitel 5* eine Sammlung von Listen und Katalogen vorgestellt und erläutert, die im Zusammenhang mit der Einführung eines ISMS und dem Einsatz des Use Case Templates hilfreich sein und verwendet werden können.
- Aufbauend auf den vorherigen Kapiteln, werden dann in *Kapitel 6* Vorschläge für die Erweiterung des UC-Templates gemacht, um eine verbesserte Nutzung voranzutreiben.

[1] Siehe auch die Seite des SINTEG-Förderprogramms auf der Homepage des BMWi https://www.bmwi.de/Redaktion/DE/Artikel/Energie/sinteg.html.

- *Kapitel 7* fasst dieses Dokument und die entsprechenden Vorschläge für die Anpassung des UC-Templates abschließend zusammen.

2 Grundlagen: Security im UC-Template

Für das Schaufensterprojekt enera wurden, teilweise bereits vor Projektbeginn, alle Anwendungsfälle im Gesamtprojekt mit dem Use Case Template (UC-Template) aus dem Standard IEC[2] 62559 systematisch erfasst. Für einen Schwerpunkt des Arbeitspakets AP12, die Informationssicherheit, erwies sich das Template allerdings als nicht ausreichend, um ein ISMS zu erstellen. Daher wurden im letzten Jahr der Projektlaufzeit Erfahrungen aus dem Projekt gesammelt, um daraus Empfehlungen für die Erweiterung des UC-Templates zu erarbeiten und in diesem Schriftstück dokumentiert. Mit diesen Empfehlungen soll das UC-Template nach IEC 62559 in der Art angepasst werden, dass Informationssicherheitsaspekte bereits bei der Anwendungsfallerfassung mitberücksichtigt und dokumentiert werden können. Somit kann in der Systementwicklung mit der Verwendung des IEC 62559 ein Security-by-Design-Vorgehen etabliert werden. Dieser Prozess sowie das angepasste Template selbst werden in diesem Dokument beschrieben und dargestellt.

Dieses Grundlagenkapitel erläutert dafür die Voraussetzungen für die Anpassung des IEC 62559 Use Case-Templates. Zunächst wird in Abschnitt 2.1 der Begriff Security-by-Design erläutert und definiert. Danach erfolgt in Abschnitt 2.2 sowohl die Beschreibung des Use Case-Templates als auch dessen Verwendung im Projekt enera. Abschnitt 2.3 beschreibt, wie die Verwendung des Use Case-Templates als Grundlage für ein Informationssicherheitsmanagementsystem (ISMS) aussehen kann. In Abschnitt 2.4 werden die Ziele der Anpassung erläutert.

2.1 Security-by-Design

Der Begriff Security-by-Design stammt ursprünglich aus dem Software-Engineering[3] und bedeutet hier, dass Software von Grund auf, also bereits im Designprozess, sicher konzipiert werden soll. Bösartige Angriffe auf das System werden generell erwartet. Bereits im Entwicklungsprozess soll von Beginn an Vorsorge getroffen werden, um Schadensauswirkungen zu minimieren – falls zum Beispiel eine Schwachstelle von Angreifern entdeckt und ausgenutzt wird.

Werden für Datenschutz und Informationssicherheit zuständige Personen, Akteure, Infrastrukturen und Schutzmaßnahmen bereits in der Planung berücksichtigt, kann dauerhaft ein höheres Schutzniveau erreicht werden. Langfristig betrachtet ist die frühzeitige Integration zudem deutlich ressourcenschonender und mit weniger Aufwand verbunden, als eine nachträgliche Integration in ein bestehendes System. Bei einer späteren Nachrüstung von Datenschutz und Informationssicherheit muss das System von den Verantwortlichen, die meist IT-Experten und

[2] IEC steht für International Electrotechnical Commission, eine internationale Standardisierungsorganisation für elektrische, elektronische und ähnliche Standards.
[3] Siehe z. B. Wikipedia.org: „Secure by Design“.

keine Domänenexperten sind, zunächst vollständig verstanden werden. Erst dann können Datenschutz und Informationssicherheit mit erheblichem Aufwand integriert werden. Außerdem kann es erforderlich sein, Datenmodelle, Infrastrukturen u. ä. komplett neu zu entwerfen, falls mit dem bestehenden System bestimmte Sicherheitsmaßnahmen nicht umgesetzt werden können. Die Kosten für möglicherweise notwendige Korrekturen im Hinblick auf Datenschutz und Informationssicherheit können somit enorme Ausmaße annehmen, je später solche Korrekturen vorgenommen werden. Grob quantifizieren lassen sich diese Fehlerkosten mit Hilfe der 10er-Regel [11]. Demnach erhöhen sich die Kosten für die Behebung eines Defizits im Bereich Datenschutz und IT-Sicherheit mit jeder späteren Phase um den Faktor 10.

Wesentliche Security-by-Design-Prinzipien sind beispielsweise:

- Minimierung der Angriffsfläche
- Nutzung sicherer Standardwerte („secure by default“)
- Prinzip der geringsten Berechtigung („least priviledge“)
- Prinzip der mehrfachen Verteidigungslinie („defense in depth“)
- Vollständige Zugriffskontrolle („complete mediation“)
- Sichere Fehlerbehandlung und Protokollierung („fail securely“)
- „Vertrau keinen IT-Services“
- Minimale gemeinsame Ressourcen („least common mechanism”)
- Trennung von Rollen
- „Keep it simple“ („economy of mechanism”)
- Sicherheitsprobleme richtig beheben

Diese Ansätze müssen bereits bei bestimmten Design-Entscheidungen berücksichtigt werden, da entsprechende Anpassungen, wie oben bereits erwähnt, gegebenenfalls hohe Kosten nach sich ziehen können. Eine detaillierte Darstellung dieser Prinzipien findet sich in Kapitel 3.4.3 des Ergebnisdokuments zu AS 12.2.4 „Governance, Compliance und Datenschutz: Erhebungen, Strukturen und Management“ [7].

Die Konzeption eines zunächst generischen ISMS im Kontext des allgemeinen System-Designs – wie bei enera umgesetzt – unterstützt diesen Security-by-Design-Ansatz. Ein wirksames ISMS ist für ein Informationssystem von hohem Stellenwert, und es kann nur auf Basis einer vollständigen und korrekten Beschreibung des (entstehenden) Systems wirksam etabliert werden.

2.2 Use Cases bei enera

Bereits in der Vorbereitungsphase des Schaufensterprojekts enera wurde beschlossen, standardisierte Use Cases gemäß dem IEC 62559 UC-Template zu den Projektaktivitäten zu erstellen und damit die Anwendungsfälle des Projektes systematisch zu erfassen. Dies erfolgte zum einen in Dokumenten im MS Word®-Format, zum anderen aber auch direkt in einem Use Case Management Repository (UCMR), das für alle Projektpartner von enera zur Verfügung stand. Das verwendete Use Case Template nach IEC 62559 ist im Anhang A.1 angefügt und wird im Folgenden in Abschnitt 2.2.1 kurz beschrieben. Anschließend folgt in Abschnitt 2.2.2

eine Vorstellung des in enera praktizierten Vorgehens, das auch in einem Erfahrungsbericht wissenschaftlich publiziert wurde [10].

2.2.1 Beschreibung des Use Case-Templates

Das UC-Template nach IEC 62559 gliedert sich in die folgenden acht Abschnitte:

1. Beschreibung des Use Cases
2. Diagramme zum Use Case
3. Technische Details
4. Schritt für Schritt Analyse
5. Ausgetauschte Informationen
6. Anforderungen
7. Übliche Bezeichnungen und Definitionen
8. Individuelle Informationen (optional)

Das erste Kapitel („*Beschreibung des Use Cases*“) sieht allgemeine Informationen zum Use Case vor, die deskriptiv erfasst werden können. Lediglich die Ziele des Use Cases (*Template-Abschnitt 1.3*) und die Key Performance Indikatoren (*Template-Abschnitt 1.5*) sollen miteinander verlinkt werden. Das zweite Kapitel („*Diagramme zum Use Case*“) ist für Diagramme vorgesehen. Hier können nicht nur High-Level Übersichten zum Use Case eingefügt werden, sondern auch Sequenzdiagramme, die als Grundlage für die später folgende Schritt-für-Schritt-Analyse dienen können.

Ab dem *dritten Template-Abschnitt* folgen die *„technischen Details*“, in denen zunächst die im Use Case beteiligten Akteure[4] (inkl. Assets[5]) und Referenzen (z. B. regulatorische Vorgaben) gelistet werden. In der „*Schritt-für-Schritt-Analyse“* in *Template-Abschnitt 4* werden die Szenarien des Use Cases und deren Szenarioschritte aufgeführt. Die dabei *„ausgetauschten Informationen“* werden in *Template-Abschnitt 5* zusammengefasst. Die in der Schritt-für-Schritt-Analyse benannten *„Anforderungen“* sind wiederum in *Template-Abschnitt 6* kategorisiert und beschrieben. Die abschließenden *Template-Abschnitte 7* (*„Übliche Bezeichnungen und Definitionen“*) und *8* (*„Individuelle Informationen“*) dienen als Glossar und für individuelle, anwendungsfall-spezifische (Zusatz-)Informationen. Ein allgemeiner Beispiel-UC mit dem aktuellen IEC 62559 Template ist im Anhang A.1 zu finden.

Der Wunsch der Weiterverwendung der Use Cases als Grundlage für die Erstellung eines ISMS begann im Laufe des Projekts. Bei der ursprünglichen Erfassung der Use Cases war diese Verwendung jedoch noch nicht berücksichtigt worden. Das UC-Template adressierte bis dahin das Thema Informationssicherheit noch nicht explizit. Somit war das Vorgehen gemäß Security-by-Design noch nicht allein mit dem UC-Template durchführbar, sondern es mussten weiteren Informationen zu den Use Cases in Bezug auf Informationssicherheit eingeholt werden.

[4] Akteure sind Systeme oder Personen, die im Kontext des Use Cases aktiv sind.
[5] Der Begriff Assets kann mit „schützenswerte Güter“ übersetzt werden. Im Sinne der Informationssicherheit und im Kontext dieses Lösungselements handelt es sich bei Assets um alle Anwendungen und Systeme, deren Standorte/Infrastruktur und deren Kommunikationsverbindungen / Netze sowie die dabei ausgetauschten Informationen.

2.2.2 Vorgehen im Projekt

Das im Projekt praktizierte Vorgehen zur Erfassung und Verwaltung der Use Cases gliederte sich insgesamt in fünf Phasen, die in Abbildung 1 dargestellt sind.

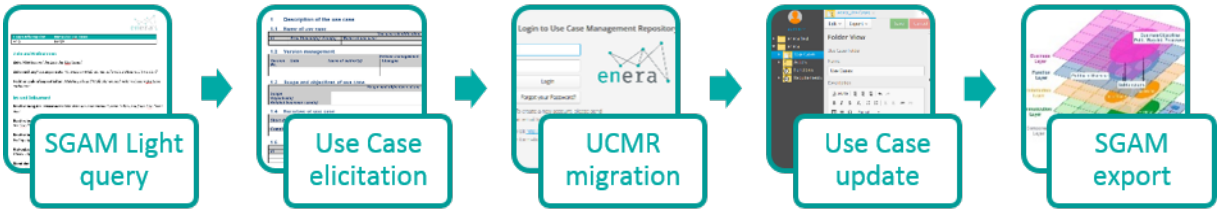


Abbildung 1: Phasen der Use Case Bearbeitung (Quelle: [10])

In der **ersten Phase** wurde eine sogenannte „SGAM[6] Light“ Abfrage gestartet, für diese wurde ein projektspezifisches Template mit Elementen aus dem regulären IEC 62559-Template genutzt. Darauf aufbauend wurden die Use Cases in der **zweiten Phase** zunächst klassifiziert und die technisch relevanten Use Cases zur weiteren Ausgestaltung ausgewählt. Diese Use Cases wurden im IEC 62559-Template als Dokumente im MS Word®-Format ausgefüllt. Zusätzlich wurde eine vorbereitete Akteursliste basierend auf dem Rollenmodell für die Marktkommunikation im deutschen Energiemarkt [12] sowie ein Akteursglossar bereitgestellt; dies geschah mit dem Ziel, die Konsistenz zwischen den einzelnen Use Cases zu verbessern. Die Akteursliste sollte dabei im Verlauf der Erfassung kontinuierlich ergänzt und abgestimmt werden.
Die Überführung der Use Cases von den MS Word® Dokumenten in das webbasierte UCMR des Projektpartners OFFIS erfolgte in der **dritten Phase**. Im Zuge dessen wurde auch ein Konsistenzcheck bei den Akteuren sowie den ausgetauschten Informationen im Rahmen von Workshops durchgeführt. Des Weiteren wurden die ausgetauschten Informationen manuell auf einen High-Level-Datenobjektkatalog abgebildet, um sie zu gruppieren.
In der **vierten Phase** wurden die Use Cases im weiteren Projektverlauf im UCMR aktualisiert und teilweise weiter verfeinert. Die so gewonnenen Use-Case-Spezifikationen dienten in der **fünften Phase** als Basis für die Dokumentation des Projekts im SGAM.

Die Weiterverwendung der Use Cases als Grundlage für ein ISMS begann während der **vierten Phase**. Bei der Erfassung der Use Cases war diese Verwendung jedoch noch nicht berücksichtigt worden. Das Use Case Template adressiert bisher nicht explizit das Thema Informationssicherheit. Es können dort allerdings bei den „Requirements“ neben weiteren Anforderungen bereits jetzt schon auch Sicherheitsanforderungen benannt werden, die dann in der Beschreibung der einzelnen Szenarioschritte referenziert werden können. Dies wurde bei der Nachbearbeitung der Use Cases für ihre Verwendung als ISMS-Grundlage auch im UCMR umgesetzt.

[6] SGAM steht für Smart Grid Architecture Model und repräsentiert ein Rahmenwerk, das für die Entwicklung von Smart Grid Systemarchitekturen verwendet wird. Siehe auch https://ec.europa.eu/energy/sites/ener/files/documents/xpert_group1_reference_architecture.pdf.

2.3 Use Cases als Grundlage für ein ISMS

Bei den Inhalten von Use Cases ist im Zusammenhang mit Security-by-Design einerseits zu fragen, ob grundsätzlich alle relevanten sicherheitsbezogenen Aspekte der Informationssicherheit – auch im Hinblick auf industrielle Angriffssicherheit – berücksichtigt wurden, und ob andererseits die Inhalte als Basis für ein ISMS hinreichend vollständig, konkret, detailliert, redundanz- und widerspruchsfrei sind.

In enera AP12 bestand eine der Aufgaben darin, ein ISMS, also ein Managementsystem für Informationssicherheit, für das Projekt enera zu erstellen. Bei der Etablierung eines ISMS sollten schon möglichst viele Informationssicherheitsthemen und -aufgaben sowie Sicherheitsanforderungen in der Planungs- und Designphase adressiert und identifiziert werden. Hierfür gibt es diverse Standards und Normen, die Vorgaben für die Einführung eines ISMS machen. Allerdings fokussieren sich solche Normen, wie z. B. die ISO/IEC 2700x-Reihe, eher auf bestehende komplexe Systeme und deren Unternehmen, sind aber nicht primär auf die Planungsphase eines Systems sowie auf Projekte mit vielen Projektpartnern zugeschnitten. Weiterhin liegt der Fokus des aktuell vorhandenen UC-Templates als Systems Engineering-Ansatz noch nicht auf Security-by-Design, also der Erfassung und Berücksichtigung von sicherheitsrelevanten Eigenschaften von Beginn an. Daher ist, um die Integration von Informationssicherheit bereits in der Planungsphase von Projekten zu ermöglichen, ein neuer Ansatz notwendig.

Somit sollen in Zukunft Informationssicherheitsaspekte im Systemdesign bereits während der Use Case Erfassung innerhalb des UC-Templates nach IEC 62559 berücksichtigt werden. Es konnten zwar im ursprünglichen Template schon über Umwege Sicherheitsanforderungen benannt werden, doch erleichtert eine explizite Adressierung von Informationssicherheit eine hinreichend vollständige und detaillierte Erfassung der relevanten Angaben zu den schützenswerten Objekten und deren Schutzbedarf bedeutend. Daher müssen Informationen, die für die Erstellung eines ISMS relevant sind, bereits direkt im UC-Template vorgesehen sein, damit sie von Beginn an erfasst werden können.

Die Use Cases im Projekt enera waren zu Projektbeginn, als sie erfasst wurden, aufgrund des Schaufenster-Charakters des Projekts teilweise noch sehr konzeptionell und erst theoretisch entworfen. Dies hatte den Vorteil, dass der Security-by-Design Ansatz tatsächlich in einer sehr frühen Design-Phase angewandt werden konnte. Die erfassten Use Cases wurden zu Scopes zusammengefasst, die jeweils den Geltungsbereich eines anteiligen ISMS bilden. In Abbildung 2 sind für enera die einzelnen Akteure aller Use Cases als grüne nummerierte Punkte sowie die einzelnen Scopes – acht Stück an der Zahl – in verschiedenen Farben und verortet im SGAM dargestellt.

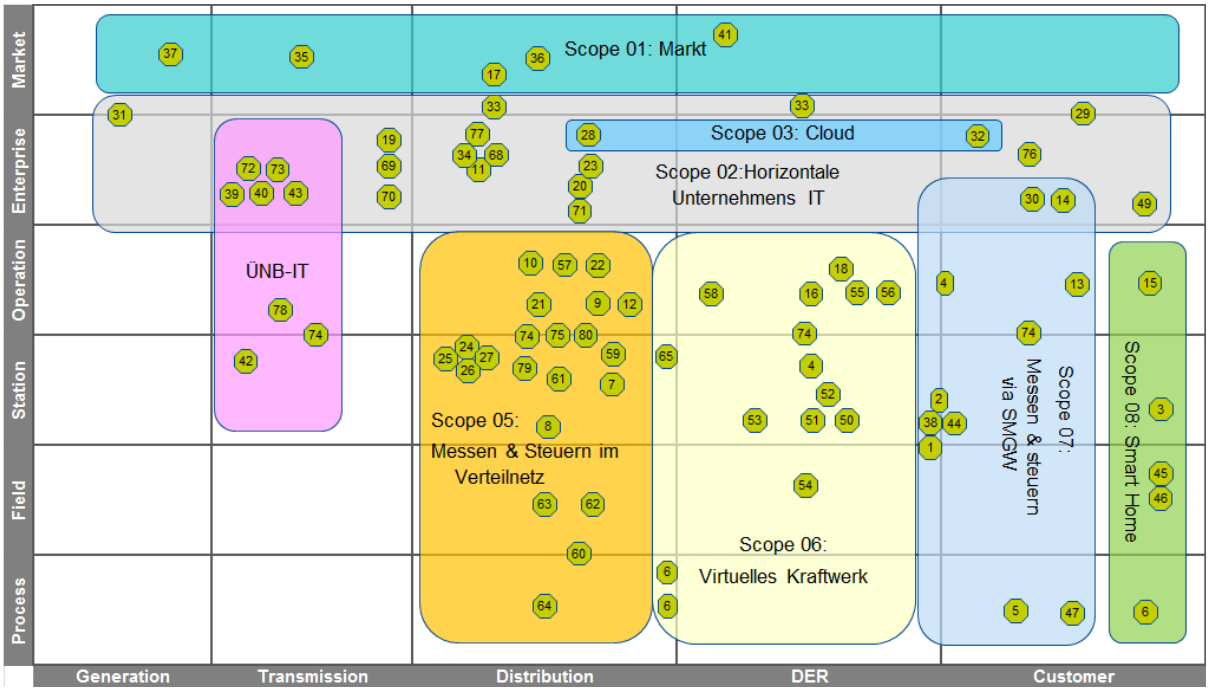


Abbildung 2: Scope-Einteilung und Use Case Akteure verortet im SGAM

Bei den Arbeitsschritten zur Erarbeitung des ISMS wurden zwei Scopes für unterschiedliche Vorgehensweisen ausgewählt:

- Vorgehen nach IT-Grundschutz mit Erstellen eines IT-Grundschutz-Profils „Virtuelles Kraftwerk“ im Scope 06 „Virtuelles Kraftwerk“.
  Basis: Use Case, der gezielt für ein IT-Grundschutzprofil erstellt wurde. Siehe hierzu auch die zu dieser Thematik erstellte Masterarbeit [9].
- Vorgehen nach IT-Grundschutz im Scope 07 „Messen und Steuern via SMGW“ (auch als „Pilot-Scope“ bezeichnet)
  Basis: Zugehörige vorhandene enera-Use Cases als Grundlage für ein generisches ISMS.

Die in Kapitel 3 beschriebene Erweiterungen beziehen sich auf den Scope 6 „Virtuelles Kraftwerk“. Die in Kapitel 4 beschriebenen Erfahrungen beziehen sich vor allem auf die Arbeiten im Scope 7 „Messen und Steuern via SMGW“.

Die zu Scope 7 zugehörigen Use Cases wurden z. T. im Projektverlauf auf Basis von Erfahrungen überarbeitet und ergänzt, die sich bei Strukturanalyse / Inventarisierung (AS 12.2.7) und Schutzbedarfsfeststellung (AS 12.2.8) für das generische ISMS im Pilot-Scope ergaben. Dieses iterative oder zirkuläre Vorgehen, dass die Use Cases als Basis für das generische ISMS dienen und daraus wiederum Ergänzungen für die Use Cases abgeleitet wurden, ist in Abbildung 3 dargestellt.

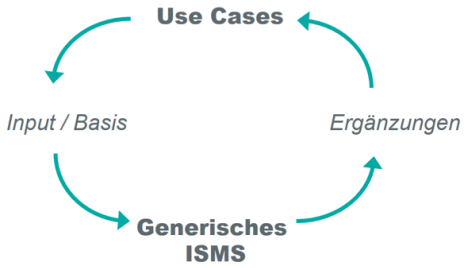


Abbildung 3: Wechselwirkung zwischen Use Cases und generischem ISMS

2.4 Ziele der Anpassungen

Bei der Etablierung eines ISMS sollten alle zugehörige Themen und Aufgaben schon in der Planungsphase adressiert werden. Insbesondere sollten die Anforderungen an die Informationssicherheit allgemein und an die konkrete Informations- und IT-Sicherheit schon in den Planungs- und Design-Phasen so vollständig und detailliert wie möglich identifiziert werden. Siehe hierzu ebenfalls Kapitel 3.7 „Durchsetzen eines kontinuierlichen Betriebs von Informationssicherheit“ im Ergebnisdokument zu AS 12.2.22 „Gap-Analyse“ [8]. Dort wird – bezogen auf den klassischen Plan-Do-Check-Act-Zyklus (PDCA), siehe Abbildung 4 – vorgeschlagen, dass die Berücksichtigung von Informationssicherheit daher von den Schritten „Check“ und „Act“ auf die Schritte „Plan“ und „Do“ ausgeweitet werden sollte.

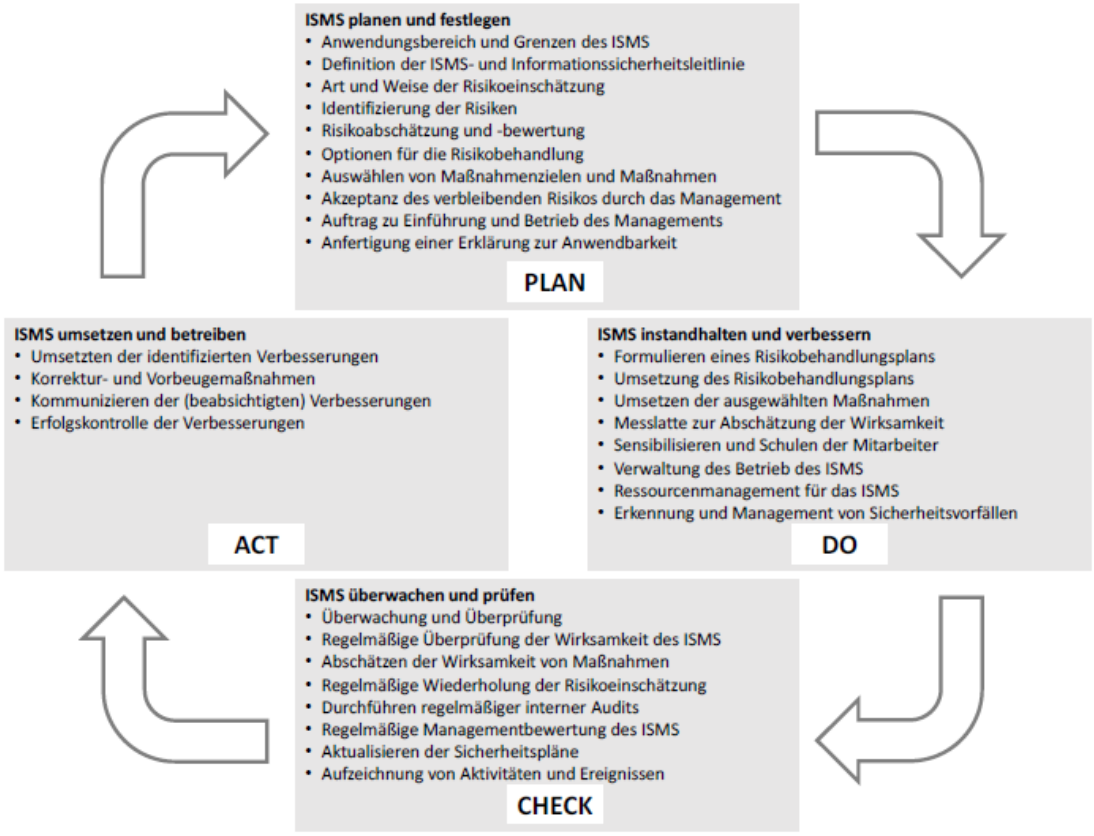


Abbildung 4: PDCA-Zyklus angelehnt an die ISO/IEC 27001 aus der Masterarbeit zur Thematik [9]

Weiterhin ist es sinnvoll die systematische Erfassung von weiteren Qualitätszielen neben der Informationssicherheit, wie bspw. Kompatibilität, Wartbarkeit oder Zuverlässigkeit, bereits zu Beginn des Entwicklungsprozesses zu integrieren, das Vorgehen hierzu ist im Ergebnisdokument AS 12.2.25, Kapitel 3.1 [14] beschrieben. Die Integration von Qualitätszielen wird ebenfalls bei der Anpassung des IEC 62559 Templates berücksichtigt.

Entsprechend den im vorliegenden Dokument beschriebenen Erfahrungen aus dem enera-Projekt und den daraus erarbeiteten Empfehlungen (siehe Kapitel 4) soll das UC-Template in der Art optimiert werden, dass Informationssicherheitsaspekte bereits von Beginn an im Entwicklungsprozess und bei der Use Case Erfassung mitberücksichtigt werden können. Dafür wurden die entsprechenden Normen und Standards wie z. B. die IEC/ISO 2700x-Reihe und der BSI-Grundschutz sowie das BSI-Grundschutzprofil herangezogen. Dabei wird auch die Vorgehensweise bei der Erarbeitung und Dokumentation von Use Cases thematisiert, die aus Sicht eines ISMS einen Informationsverbund bilden und die daher im Zusammenhang gesehen werden müssen.

3 Integration BSI IT-Grundschutz in UC-Template

In diesem Kapitel wird gezeigt, wie Informationssicherheit im aktuellen, noch nicht angepassten UC-Template integriert werden konnte. Dafür wird ein beispielhafter Use Case für ein Virtuelles Kraftwerk aus dem Projekt verwendet. Als Basis dafür diente das Vorgehen für ein BSI IT-Grundschutzprofil[7].

Zur Vorbereitung eines IT Grundschutz Profils nach Vorgaben des BSI über datentechnische Betriebsabläufe in einem virtuellen Kraftwerk wurde ein zugehöriger Use Case erstellt. Dafür wurde das etablierte Use Case-Template und das enera-UCMR Repository verwendet. Anhand dieses Anwendungsfalls sollten Informationen, um eine anschließende Sicherheitsanalyse und die Erstellung des IT-Grundschutzprofils zu ermöglichen, mit dem Template erfasst werden. Da jedoch nicht alle Informationen, die für ein IT Grundschutz-Profil erforderlich sind, eindeutig einzelnen Abschnitten im etablierten UC-Template zugeordnet werden konnten, wurde eine systematische Zuordnung der für den IT Grundschutz relevanten Informationen zu denen im UC-Template, wie in folgender Tabelle 1 dargestellt, vorgenommen.

IT-Grundschutz	**UC-Template**
Geschäftsprozesse und zugehörige Informationen	Scenarios (UC-Template Abschnitt 4.2), Information exchanged (UC-Template Abschnitt 5) und Requirements (UC-Template Abschnitt 6)
Anwendungen	Actor Group (UC-Template Abschnitt 3.1)
Zuordnung Anwendungen zu Geschäftsprozesse	Nennung in mindesten einem Szenarioschritt des Geschäftsprozess (UC-Template Abschnitt 4.2)
Zuordnung Anwendungen zu Systemen	Definition aller Systeme, die einer Anwendung zugeordnet sind als Actor Group (UC-Template Abschnitt 3.1)
IT-Systeme	Actor Typ IT-System (UC-Template Abschnitt 3.1)
Industrielle IT	Actor Typ Industr. IT (UC-Template Abschnitt 3.1)
Zuordnung Systeme zu Infrastruktur	Nennung der Infrastruktur in der Actor-Spalte „Further information specific to this use case“ (UC-Template Abschnitt 3.1)
Infrastruktur: Gebäude, Räume, Gelände	Custom Information (UC-Template Abschnitt 8)

[7] In einem IT-Grundschutz-Profil werden die Schritte eines Sicherheitsprozesses für einen bestimmten Anwendungsbereich beispielhaft als Mustervorlage beschrieben. Es kann als Grundlage für den Aufbau eines Informationsmanagementsystems (ISMS) dienen. Methodische Anleitung und Beispiele siehe https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Profile/it-grundschutz-profile_node.html.

IT-Grundschutz		**UC-Template**
Zuordnung der Systeme zu den Netzen / Kommunikationsverbindungen	Interne Netze und Verbindungen	Beschreibung des Informationsaustausches von jeweils zwei angeschlossenen Systemen und Referenzieren auf Netze / Kommunikationsverbindung als Requirement (UC-Template Abschnitt 4.2 & 6)
	Außenverbindungen	Beschreibung als zwei aufeinander folgende Szenarioschritte (UC-Template Abschnitt 4.2) 1. Sendersystem an Außenverbindung 2. Außenverbindung an Empfängersystem
Netze und Kommunikation	Außenverbindungen	Actor der Actor Group NET / Außenverbindung (UC-Template Abschnitt 3.1)
	Interne Netze und Verbindungen	Requirement der Category COM (UC-Template Abschnitt 6)

Tabelle 1: Zuordnung von Bestandteilen des IT-Grundschutzprofils im UC-Template

Im Rahmen der Schutzbedarfsfeststellung im IT-Grundschutz wird der Schutzbedarf zunächst für die *Geschäftsprozesse* und zugehörigen Informationen bestimmt. Deren Schutzbedarf vererbt sich dann auf die *Anwendungen, IT-Systeme, Räume* und *Kommunikationsverbindungen*. Daher müssen die Geschäftsprozesse und zugehörigen Informationen, Anwendungen, IT-Systeme, Räume und Kommunikationsverbindungen im Use Case abgebildet werden. Für den hier auszugsweise vorgestellten Use Case wurde dabei das vorhandene UC-Template ohne technische Anpassungen im UCMR verwendet, der komplette Use Case ist im Anhang A.2 dargestellt.
In den folgenden Abschnitten werden Beispiele für die Verwendung der einzelnen Abschnitte des ursprünglichen UC-Templates, für „Geschäftsprozesse und zugehörige Informationen“, für „Anwendungen, IT-Systeme und Räume“ sowie für „Kommunikationsverbindungen“ anhand des entsprechenden UCs für ein virtuelles Kraftwerk gegeben. Nur an einer Stelle war hierfür eine kleine Anpassung notwendig.

3.1 Geschäftsprozesse und zugehörige Informationen

Die Geschäftsprozesse werden im UC-Template über die Szenarien („*Scenarios*“) modelliert, siehe Tabelle 2, die zugehörigen Informationen sind dann die ausgetauschten Informationen („*Information exchanged*“) in den einzelnen Schritten, siehe Tabelle 3. Der Schutzbedarf wurde im vorliegenden Use Case bereits bei den ausgetauschten Informationen (UC-Template Ab-

schnitt 5) dokumentiert („*Requirements-IDs*“), wobei hier auch die Begründung für die Einschätzung ergänzt wurde. Diese in Rot markierte Spalte wurde im vorliegenden Beispiel ergänzt, da sie für den IT-Grundschutz benötigt wird, aber im standardisierten UC-Template nicht vorgesehen ist. Die Anforderungen selbst sind dann in UC-Abschnitt 6 („*Requirements*“) definiert. Das UC-Template arbeitet, wie gerade beschrieben, im Allgemeinen viel mit Verweisen, dies ist auch in den hier dargestellten Tabellen (Tabelle 2, Tabelle 3 und Tabelle 4) zu sehen. Die im folgenden Beispiel verwendeten Akteure sind das DER[8] SCADA[9] System (Sys-CC-1) und die Switche[10] der Leitwarte[11] (Sys-CC-7), die wiederum im UC-Template-Abschnitt 3.1 bei den Akteuren definiert sind.

4.2 Steps – Scenarios

Scenario								
Scenario Name:		Standardbetrieb (Planung und Steuerung) des virtuellen Kraftwerks						
Step No.	***Event***	***Name of process/ activity***	***Description of process/ activity***	***Service***	***Information producer (actor)***	***Information receiver (actor)***	***Information exchanged (IDs)***	***Requirements R-ID***
x	Neuer Sollwert für DER Anlage berechnet	Sollwertbefehl senden	Senden des neuen Sollwerts zur DER Anlage	CHANGE	SYS-CC-1	SYS-CC-7	DER-Sollwert	NET-CC-4

Tabelle 2: Abschnitt 4.2 des UC-Templates: Steps-Scenarios

5 Information Exchanged

Information Exchanged				
Information exchanged ID	***Name of information***	***Description of information exchanged***	***Requirements IDs***	***Reason for protection level*** ***According to security goals availability (SLA), integrity (SLI) and confidentiality (SLC)***
DER-Sollwert	DER-Sollwert	Sollwert für die erzeugte oder verbrauchte Leistung einer DER Anlage.	SLA-high; SLI-high; SLC-normal	Kritische Funktionalität aber unkritische Privatsphäre, da M2M Kommunikation

Tabelle 3: Abschnitt 5 des UC-Templates: Information Exchanged

[8] DER steht für Dezentrale Energieressource.
[9] SCADA steht für Supervisory Control and Data Acquisition. Ein SCADA System stellt ein System dar, das technische Prozesse überwacht und steuert.
[10] Ein Switch ist ein Gerät, das die Kommunikation in Computernetzen steuert.
[11] Eine Leitwarte (auch Leitstand) ist eine technische Einrichtung, die Menschen bei der Überwachung und Steuerung von Prozessen unterstützt.

6 Requirements (optional)

Categories ID	Category name for requirements	Category description
NET	Netzwerke & Kommunikation	Diese Kategorie gibt Informationen über die genutzten IT-Netzwerke.
SLC	Schutzbedarf der Vertraulichkeit gemäß IT-Grundschutz	Einschätzung der Schadenshöhe bei Verletzung des Grundwertes Vertraulichkeit.
SLI	Schutzbedarf der Integrität gemäß IT-Grundschutz	Einschätzung der Schadenshöhe bei Verletzung des Grundwertes Integrität.
SLA	Schutzbedarf der Verfügbarkeit gemäß IT-Grundschutz	Einschätzung der Schadenshöhe bei Verletzung des Grundwertes Verfügbarkeit.
Requirement ID	**Requirement name**	**Requirement description**
NET-CC-4	Intra-center Integration Bus	Communication hub in einem Control Center
SLC-normal	Normale Vertraulichkeit	Einschätzung der Anforderungen an die Vertraulichkeit ist normal: Die Schadensauswirkungen bei Verletzung der Vertraulichkeit sind begrenzt und überschaubar.
SLI-high	Hohe Integrität	Einschätzung der Anforderungen an die Integrität ist hoch: Die Schadensauswirkungen bei Verletzung der Integrität können beträchtlich sein.
SLA-high	Hohe Verfügbarkeit	Einschätzung der Anforderungen an die Verfügbarkeit ist hoch: Die Schadensauswirkungen bei Verletzung der Verfügbarkeit können beträchtlich sein.

Tabelle 4: Abschnitt 6 des UC-Templates: Requirements (optional)

3.2 Anwendungen, IT-Systeme und Räume

Anwendungen sind im UC-Template den Akteuren (UC-Template Abschnitt 3.1) zuzuordnen, weiterhin gibt es allgemein die Möglichkeit zur Gruppierung von Akteuren. Entsprechend wurde dies genutzt, um Akteure Anwendungen zuzuordnen. Die im vorherigen Auszug genutzten Akteure DER SCADA System (Sys-CC-1) und Switche der Leitwarte (Sys-CC-7) gehören beispielsweise zum Kontroll- und Steuerungssystem bzw. zur Netzdienste-, Benutzer- und Ressourcenverwaltung, siehe Tabelle 5.

Anwendungen sollen gemäß IT-Grundschutz **IT-Systemen** zugeordnet werden. Diese Zuordnung von IT-Systemen zu Anwendungen erfolgte im UC-Template durch die Gruppierung der Anwendungen und den „*Actor type*“, dies ist ebenfalls in Tabelle 5 zu sehen.

Für die Zuordnung von **Räumen** wurde im Beispiel-UC das Feld der „*Further information*“ im UC-Template Abschnitt 8 in Verbindung mit den „*Custom information*“ genutzt, da dies im UCMR eine passende Modellierung zuließ, dies ist in den beiden bereits referenzierten Tabellen (Tabelle 5 und Tabelle 6) insgesamt zu sehen.

3.1 Actors

Actors			
Grouping (Community)		**Group description**	
ANW-3		Kontroll- und Steuerungssystem	
Actor name	**Actor type**	**Actor description**	**Further information specific to this use case**
SYS-CC-1	IT-System	DER SCADA System	[INF-CC-2] Serverraum
IND-DER-1	Industr. IT	Device Energy Management	[INF-DER-2] Betriebsgebäude DER-Anlage
Grouping (Community)		**Group description**	
ANW-4		Netzdienste, Benutzer- und Ressourcenverwaltung	
Actor name	**Actor type**	**Actor description**	**Further information specific to this use case**
SYS-CC-5	IT-System	Domain Controller Leitwarte	[INF-CC-2] Serverraum
SYS-CC-7	IT-System	Switche Leitwarte	[INF-CC-2] Serverraum

Tabelle 5: Abschnitt 3.1 des UC-Templates: Actors

8 Custom information (optional)

Custom information (optional)		
Key	**Value**	**Refers to section**
INF-DER-2	Betriebsgebäude DER-Anlage (enthält DER Gateway, Device Energy Management)	3.1 Actors
INF-CC-2	Serverraum im Unternehmensgebäude (enthält Energy Management System, Forecasting System for the Generation of Renewable Energy Units, DER SCADA System)	3.1 Actors

Tabelle 6: Abschnitt 8 des UC-Templates: Custom Information (optional)

3.3 Kommunikationsverbindungen

Die Kommunikationsverbindungen zwischen den Akteuren werden immer beim Austausch von Informationen in den Szenarioschritten genutzt. Da das UC-Template bei den Szenarioschritten alle Spalten vorgegeben hat, musste eine der vorhandenen für die Dokumentation der Kommunikationsverbindung genutzt werden. Dafür hat sich die „Requirements“-Spalte angeboten, sodass die Kommunikationsverbindungen eine „Requirements Category“ bilden, siehe Tabelle 7 und Tabelle 8.

4.2 Steps – Scenarios

Scenario								
Scenario Name:	Standardbetrieb (Planung und Steuerung) des virtuellen Kraftwerks							
Step No.	**Event**	**Name of process/ activity**	**Description of process/ activity**	**Service**	**Information producer (actor)**	**Information receiver (actor)**	**Information exchanged (IDs)**	**Requirements R-ID**
x	Neuer Sollwert für DER Anlage berechnet	Sollwertbefehl senden	Senden des neuen Sollwerts zur DER Anlage	CHANGE	SYS-CC-1	SYS-CC-7	DER-Sollwert	NET-CC-4

Tabelle 7: Abschnitt 4.2 des UC-Templates: Steps - Scenarios

6 Requirements (optional)

Categories ID	Category name for requirements	Category description
NET	Netzwerke & Kommunikation	Diese Kategorie gibt Informationen über die genutzten IT-Netzwerke.
Requirement ID	**Requirement name**	**Requirement description**
NET-CC-4	Intra-center Integration Bus	Communication hub in einem Control Center

Tabelle 8: Abschnitt 6 des UC-Templates: Requirements (optional)

4 Ableitung von Empfehlungen aus enera Erfahrungen für die Anpassung des UC-Templates

Im Rahmen der Use-Case Bearbeitung und insbesondere der Weiterverarbeitung in den Phasen der Sicherheitsanalyse – wie der „Strukturanalyse und Inventarisierung“, der „Schutzbedarfsfeststellung“ und der „Risikoanalyse“ – wurden einige Erfahrungen im Rahmen des Projekts enera für Verbesserungspotenzial des UC-Templates gesammelt, die dann im letzten Projektjahr aufgearbeitet und dann in diesem Ergebnisbericht dokumentiert wurden. Die Erfahrungen werden in den folgenden Abschnitten 4.1 bis 4.4 anhand allgemeiner Erfahrungen und der beschriebenen Phasen des Projekts erläutert.
In Bezug auf Security-by-Design lassen sich aus den Erfahrungen eine Reihe an Empfehlungen für die Use Case Erfassung mit dem IEC 62559-Template ableiten. Diese Empfehlungen sollen dann bei der Systementwicklung auch eine höhere Detaillierung und eine höhere UC-übergreifenden Konsistenz der Inhalte bezwecken. In Abschnitt 4.5 werden aus den Erfahrungen Empfehlungen für die Bearbeitung von Use Cases und eine Anpassung des Use Case-Templates hinsichtlich Security-by-Design abgeleitet.

4.1 Allgemeine Erfahrungen bei der Erfassung von Use Cases

Bereits bei der vorherigen Sammlung, Konsolidierung und Überführung der Use Cases in das UCMR wurden unter anderem methodische Erfahrungen gemacht, die auch hinsichtlich Security-by-Design hilfreich sind. Diese wurden im veröffentlichten Erfahrungsbericht [10, Kapitel 3 S. 5 ff.] bereits dokumentiert. Von den methodischen Erfahrungen aus [10] sind folgende Erfahrungen auch für die Use Cases als Grundlage für ein ISMS relevant, auch wenn sie nicht zwingend zu einer Anpassung oder Detaillierung der Use-Case-Methodik führen:

- Es wurden gute Erfahrungen mit einem **inkrementellen Ausfüllen des Use Case-Templates** gemacht (es gab zunächst ein „SGAM Light“, bevor die eigentlichen Use Cases erfasst wurden). Die Erfassung von Use Cases sollte also in mehrere Phasen gegliedert werden, in denen vorgegeben ist, welche Informationen im Use Case jeweils ergänzt werden sollen. Dies hat zum einen den Vorteil, dass die Erfassung der Use Cases in kleinere Aufgaben mit jeweils gut überschaubarem Aufwand gegliedert werden. Zum anderen kann und sollte nach den einzelnen Phasen jeweils konsolidiert werden, ob die Informationen in der vorliegenden Form konsistent zueinander sind und den Ansprüchen des Projekts genügen. Letzteres kommt vor allem in Projekten mit vielen Stakeholdern zum Tragen.
- Bei der Größe des Projektes enera wurden insgesamt 70 Use Cases identifiziert, von denen 50 ausführlicher beschrieben wurden. Bei dieser Vielzahl an Use Cases gab es sehr große **Unterschiede in der Granularität** der Use Cases, da sie sich aufgrund des Projektcharakters auch in unterschiedlichen Entwicklungsstadien befanden (konzeptionelle Ideen vs. Test von Prototypen). Entsprechende unterschiedliche Entwicklungsstadien sollten rechtzeitig adressiert, der zugehörige Umgang frühzeitig geklärt und das Entwicklungsstadium klassifiziert und dokumentiert werden.

- Bei der Erfassung von Use Cases mittels des vorgegebenen **Templates in *MS Word***, welches nicht schreibgeschützte Formulare verwendet, können **methodische Vorgaben durch den Nutzer ignoriert** werden. Es wurden teilweise Informationen an Stellen notiert, die nicht zum eigentlichen Template gehören und daher beim Import in das UCMR nicht einfach übernommen werden konnten. Daher empfiehlt sich – gerade wenn übergreifende Listen verwendet und Bezüge zwischen einzelnen Feldern hergestellt werden sollen – die **Verwendung eines UCMRs von Beginn an**, so dass methodische Vorgaben wie bspw. eindeutige, konsistente IDs durch die Implementierung des Repositories direkt erzwungen werden können. Hierbei entfällt ebenfalls der zusätzliche Schritt des Datenimports.
- Der Einsatz **übergreifender Akteurslisten** wurde angestrebt, sie wurden jedoch nicht in der gewünschten Intensität genutzt (Grund u. a. waren auch hier wieder die „Freiheiten“, die das *MS Word*-Template ließ). Beim Einsatz übergreifender, allgemeiner Listen sollte immer die Möglichkeit eigener Ergänzungen / Spezifizierungen bestehen, um Use-Case-Ownern das Dokumentieren mit eigenen Begrifflichkeiten zu ermöglichen, da sich hier Manche mit der Verwendung allgemeiner Bezeichnungen schwer tun. Des Weiteren wurden die *Akteure* und die *ausgetauschten Informationen* aus den Use Cases jeweils in einem **Konsolidierungsworkshop** überprüft, vereinheitlicht und zusammengefasst, was zu einer Verbesserung der Use Cases und damit auch zu höherer Akzeptanz übergreifender Listen führen kann. Die **Schreibrechte auf übergreifende Listen** sollten darüberhinaus sehr eingeschränkt sein, da die Owner einzelner Use Cases nicht unbedingt die Auswirkungen von Änderungen auf andere Use Cases abschätzen können. Für individuelle Änderungen empfehlen sich stattdessen Schreibrechte auf Use-Case-spezifische Ergänzungen, die jedoch nicht die allgemeinen Informationen eines Akteurs oder dergleichen beeinflussen.

4.2 Erfahrungen aus der Strukturanalyse und Inventarisierung

Die Strukturanalyse ist der erste Schritt auf dem Weg zu einem ISMS: Zuerst müssen alle Assets identifiziert werden, die zum Scope – also dem Geltungsbereich – des ISMS gehören. Dabei handelt es sich neben physischen Assets wie Infrastruktur, Servern und Netzen, auch um Software, Informationen und Prozesse. Sie alle müssen vollständig, so kleinteilig wie nötig (um z. B. beim Schutzbedarf differenzieren zu können) und so zusammengefasst wie möglich (um die Anzahl der Assets überschaubar zu halten), eindeutig benannt und ausreichend ausführlich beschrieben werden, dass alle für das ISMS relevanten Eigenschaften und Beziehungen (wie Schnittstellen, verarbeitete Informationen, Owner) ersichtlich sind.

Die Informationen zu den Assets im Pilot-Scope waren in den vorhandenen Use Cases vielfach schon vorhanden, mussten aber zum Teil noch überarbeitet und ergänzt werden.

Einige Assets waren in den Use Cases gar nicht berücksichtigt und wurden nur im enera-ISMS-Tool ergänzt. Die Informationen in den Use Cases waren nämlich zunächst nicht bzw. nicht ausreichend im Hinblick darauf erstellt worden, dass sie auch als Grundlage für ein übergreifendes ISMS dienen sollten.

In den enera Use Cases werden die IT-Systeme und die Anwendungen nicht – wie von der IT-Grundschutz-Methodik vorgegeben – als unterschiedliche Akteure dargestellt, sondern die Anwendungen werden auf den Systemen als implizit inbegriffen aufgefasst. Eine nachträgliche Änderung der Modellierung wäre mit großem Aufwand und vielen zu berücksichtigenden Nebenwirkungen verbunden, daher wurde im Projekt enera darauf verzichtet. Da es sich weitgehend um IT-Systeme mit spezifischem Einsatzzweck handelt, deren zugehörige Anwendungen entsprechend herleitbar sind, war die Zuordnung der relevanten IT-Grundschutz-Bausteine bei der IT-Grundschutz-Modellierung auch auf dieser Basis möglich. Grundsätzlich sollte die Beschreibung in den Use Cases aber so differenziert sein, dass keine nachträgliche oder zusätzliche Aufteilung der Assets / Akteure unter Sicherheitsaspekten mehr erforderlich ist.

4.3 Erfahrungen aus der Schutzbedarfsfeststellung

Bei den ersten Arbeiten für die Schutzbedarfsfeststellung der Assets im Pilot-Scope zeigte sich, dass die Strukturierung der Informationsobjekte und weiterer Assets noch stärker differenziert und vereinheitlicht werden musste, um die Schutzbedarfszuordnung und die Vererbung des Schutzbedarfes zu ermöglichen oder zu vereinfachen. Entsprechende Empfehlungen finden sich in Kapitel 6 des Ergebnisdokumentes zum AS 12.2.8 [3], die auch aus Sicht des Security-by-Design-Ansatzes sinnvoll sind.

Zur Vereinheitlichung der Informationsobjekte wurden diese durch eine nachträgliche Zuordnung zu sogenannten High-Level InfoObjekten zusammengefasst, da die Informationsobjekte an sich teilweise sehr ähnlich, aber nicht einheitlich waren. Für jedes High-Level InfoObjekt wurde zu jedem Schutzziel die Einstufung mit Begründung festgelegt, die dann wie in Abbildung 5 dargestellt auf die Informationsobjekte und weiter auf die zugehörigen Anwendungssysteme, Infrastruktur, Netze und Kommunikationsverbindungen vererbt wurde, wobei Abweichungen im Einzelfall mit entsprechenden Begründungen möglich sind.

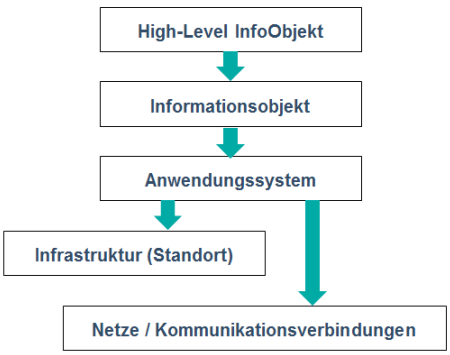


Abbildung 5: Vererbung des Schutzbedarfes - Schematische Darstellung

Auch hier sei noch einmal der bereits oben genannten Aspekt betont, dass Assets UC-übergreifend nur einmal „existieren“ und verwendet werden sollen, statt z. B. gleichartige Assets

mehrfach unter leicht unterschiedlichen Bezeichnungen einzuführen. Je weniger aussagekräftig die Beschreibungen der Assets sind, desto schwerer ist es, solche Redundanzen rechtzeitig zu erkennen und zu beseitigen.

4.4 Erfahrungen aus der Risikoanalyse

Bei der Risikoanalyse im Pilot-Scope war es immer wieder sehr wichtig, die jeweils für ein Asset und dessen initiale Konfiguration, Administration und Nutzung die verantwortlichen Akteure genau und vollständig zu kennen, um Herkunft und Auswirkungen von Gefährdungen möglichst gut bestimmen und abgrenzen zu können: Wer ist z. B. jeweils für Beschaffung, Einbau, Initialisierung und Betrieb von CLS, mME, Zählerkästen, Verkabelung und dergleichen zuständig? Diese Akteure und ihre Zuständigkeiten (und entsprechend die „Reichweite“ des jeweiligen ISMS) waren in den Use Cases noch nicht überall hinreichend detailliert abgebildet. Entsprechende Empfehlungen finden sich in Kapitel 8 des Ergebnisdokumentes zu den AS 12.2.9 und 12.2.10 [4], die auch aus Sicht des Security-by-Design-Ansatzes sinnvoll sind.

Hier wurde auch noch einmal das oben bereits genannte Erfordernis deutlich, sämtliche relevanten Assets in die UC aufzunehmen und zu beschreiben. Falls diese noch nicht genau bekannt sind, können zunächst Platzhalter-Assets verwendet werden, so dass aber zumindest Schnittstellen und zugehörige Beziehungen dokumentiert werden können.

In allen Arbeitsschritten ergaben sich einige weitere sicherheitsrelevante Erkenntnisse durch Nachfragen zu Vermutungen und Hypothesen, die auf Basis der Use Cases allein nicht geklärt werden konnten. Dies betrifft insbesondere implizit getroffene Annahmen und Voraussetzungen, die im Use Case nicht dokumentiert wurden.

4.5 Ableitung von Empfehlungen

Anhand der gewonnenen Erfahrungen aus der Strukturanalyse und Inventarisierung, Schutzbedarfsfeststellung sowie der Risikoanalyse lassen sich in Bezug auf Security-by-Design eine Reihe an Empfehlungen für die Erfassung von Use Cases mittels des IEC 62559-Templates ableiten. Diese Empfehlungen lassen sich in die folgenden drei Kategorien gruppieren: „Dokumentation“, „Ergänzende Informationen“ und „Organisatorisch“.

4.5.1 Empfehlungen zur Dokumentation

Die Empfehlungen zur Dokumentation beziehen sich im Kern alle darauf, dass **alle relevanten Assets, Eigenschaften und Beziehungen** in den Use Cases aufgenommen und detailliert beschrieben werden. Aus der Beschreibung sollen insbesondere verarbeitete Informationen, Beziehungen, Schnittstellen und entsprechende Verantwortliche ersichtlich werden, um in der weiteren Analyse für ein ISMS nach IT-Grundschutz Nacharbeiten zu ersparen. Wie bei den ergänzenden Informationen in Abschnitt 4.5.2 aufgegriffen wird, geht dies mit der eindeutigen Benennung der Assets zur Herstellung von Bezügen und der Information einher, ob personenbezogene Informationen oder andere Inhalte mit erhöhtem Schutzbedarf verarbeitet werden müssen.

- Security-by-Design-Empfehlung E-Dok-01:
  Alle für ein ISMS relevanten **Assets und Assettypen** sind aufzunehmen. Siehe hierzu z. B. die Strukturanalyse für den generischen Use Case VPP im Ergebnisdokument AS 12.2.7 [2], Kapitel 5.2.
- Security-by-Design-Empfehlung E-Dok-02:
  Die **Abhängigkeiten und Beziehungen zwischen Assets** möglichst vollständig beschreiben. Nur dann ist z. B. ersichtlich, auf welche weiteren Assets sich der Schutzbedarf eines Assets auswirkt bzw. vererbt wird.
- Security-by-Design-Empfehlung E-Dok-03:
  Alle **Rollen / Akteure und ihre Zuständigkeiten** sind so vollständig wie möglich zu beschreiben. Hierzu gehört insbesondere, welcher Akteur für welches Asset verantwortlich ist (Owner). Diese Angaben sind als Grundlage für Risikoanalysen sowie für Risikobehandlung, Maßnahmen-Umsetzung und deren Nachverfolgung wesentlich.
- Security-by-Design-Empfehlung E-Dok-04:
  Die Security-Ziele sollten bereits möglichst vollständig nach den bis dahin bekannten Systeminformationen beschrieben werden. Dies erleichtert es, den Fokus auf relevante Informationen zu behalten. Ein Verfahren zur systematischen Ableitung der Ziele und deren Nachverfolgung durch den UC ist im Dokument „Assurance Cases als Leitfaden für die Use-Case-Erhebung“ [11] beschrieben.

4.5.2 Empfehlungen zur Ergänzung von Informationen

Die nachfolgenden Empfehlungen behandeln zusätzliche Informationen neben der detaillierten Beschreibung, die größtenteils über zusätzliche, neue Felder im Use Case-Template realisiert werden können. Die konkreten Umsetzungsvorschläge dazu folgen in Kapitel 6.

- Security-by-Design-Empfehlung E-Inf-01:
  Alle Security-Ziele sowie Assets sollten einen **eindeutigen, leicht ersichtlichen Identifikator** tragen. Eine Information zur Art des Assets (Information, System, …) im Identifikator trägt zur Übersichtlichkeit bei.
- Security-by-Design-Empfehlung E-Inf-02:
  Die Beschreibung eines Assets und des zugehörigen Kontexts sollte Angaben darüber enthalten, **ob personenbezogene Informationen** oder andere Inhalte mit **erhöhtem Schutzbedarf** verarbeitet werden.
- Security-by-Design-Empfehlung E-Inf-03:
  Die **explizite Darstellung aller getroffenen Annahmen und Voraussetzungen im UC** ist wichtig**,** da hierzu sonst ein Vorwissen erforderlich wäre, das nicht vorausgesetzt werden kann. Implizite Annahmen – z. B. hinsichtlich Zuständigkeiten oder bereits getroffener Sicherheitsmaßnahmen – fallen naturgemäß nicht sofort auf, können aber indirekt erhebliche Auswirkungen haben.
- Security-by-Design-Empfehlung E-Inf-04:
  Alle Annahmen und Kontextinformationen sollen mit einem eindeutigen Identifikator versehen und durch Verweise ihren jeweiligen Security-Zielen, Szenarioschritten oder anderen UC-Elementen zugeordnet werden.

- Security-by-Design-Empfehlung E-Inf-05:
  Bei der Übersicht der Use-Case-Szenarien (Template-Abschnitt 4.1) sollte auf die Ausgangsziele verwiesen werden, um eine Rückverfolgbarkeit zu gewährleisten.
- Security-by-Design-Empfehlung E-Inf-06:
  Abweichungen vom Nominalverhalten können als Alternativszenarien im Use Case beschrieben werden. Ein Verweis auf ein jeweiliges Alternativszenario ermöglicht die schnelle Verfolgbarkeit. Dies kann beispielsweise durch eine weitere Spalte im Use-Case-Template im Template-Abschnitt 4.2 erfolgen.
- Security-by-Design-Empfehlung E-Inf-07:
  Werden Anforderungen an spezifische Systemteile abgeleitet, sollten zum Zwecke der Rückverfolgbarkeit eine Zugehörigkeit zu den Ausgangszielen dargestellt werden. Die Zuordnung könnte in einer zusätzlichen Spalte im Template-Abschnitt 6 (»Requirements«) erfolgen.

Die nachfolgenden Empfehlungen beziehen sich auf ergänzende Informationen, die bei der Erstellung der Use Cases berücksichtigt werden sollten.

- Security-by-Design-Empfehlung E-Inf-08:
  Ein **UC-übergreifender Anforderungskatalog**, in dem alle, für die Erstellung eines ISMS, relevanten Anforderungsarten gelistet und definiert sind. Dies kann dabei helfen, implizite Voraussetzungen zu erkennen und diese im UC zu dokumentieren.
- Security-by-Design-Empfehlung E-Inf-09:
  Ein **UC-übergreifendes Asset-Repository**, in dem alle Assets jeweils nur an einer Stelle eindeutig benannt und beschrieben sind, sollte während der UC-Spezifikation angelegt und genutzt werden. Dies betrifft sowohl ein Repository für die **Akteure** als auch für die **Informationsobjekte** und den bereits in E-Inf-08 angesprochenen **Anforderungskatalog**. Bei der Erstellung und der Namensgebung könnte man sich z. B. an der Smart Grid Standards Map[12] orientieren. Bei Verwendung der Assets in einzelnen UCs kann innerhalb dieses Repositories dann mit Referenzen gearbeitet werden, was zum einen die Disziplin bei der Einheitlichkeit der Namensgebung erhöht und zum anderen bei nachträglichen Änderungen viel Aufwand erspart. Des Weiteren kann bei einem übergreifenden, allgemeinen Asset Repository bei der späteren Schutzbedarfsanalyse auf bereits vorhandene Erfahrungen zur Schutzbedarfsfeststellung der Assets zurückgegriffen werden.
- Security-by-Design-Empfehlung E-Inf-10:
  Ein Assurance Case kann bei der Use-Case-Erhebung als Leitfaden für die Aktivitäten dienen und so eine höhere Vollständigkeit gewährleisten. Ein Muster-Assurance Case wird im Dokument „Assurance Cases als Leitfaden für die Use-Case-Erhebung“ [11] vorgestellt.

[12] Siehe http://smartgridstandardsmap.com/.

4.5.3 Empfehlungen zur organisatorischen Bearbeitung

Die Empfehlungen zur organisatorischen Bearbeitung basieren sowohl auf den Erfahrungen aus der „Strukturanalyse und Inventarisierung“, der „Schutzbedarfsanalyse“ und der „Risikoanalyse“, als auch aus den methodischen Erfahrungen der Use-Case-Bearbeitung an sich. Hierbei geht es vor allem um das Vorgehen bei der Erfassung und dem Management von Use Cases.

- Security-by-Design-Empfehlung E-Org-01:
  Das Projekt sollte möglichst eine **UC-übergreifende Redaktion** einsetzen, um Lücken oder Widersprüche zwischen unterschiedlichen UCs identifizieren und zu beheben. Diese Redaktion sollte auch zu Beginn direkt den Umgang mit Use Cases unterschiedlicher Granularität und unterschiedlichen Reifegrads besprechen und ein einheitliches Vorgehen beschließen.
- Security-by-Design-Empfehlung E-Org-02:
  Use Cases sollten inkrementell in **mehreren Phasen erfasst werden.** Nach jeder Iteration sollten die teilausgefüllten UC-Beschreibungen von der UC-übergreifenden Redaktion aus E-Org-01 konsolidiert werden, ehe die Beschreibungen der nächsten Phase weiter vervollständigt werden.
- Security-by-Design-Empfehlung E-Org-03:
  Use Case Management Repositories sollten von Beginn an genutzt werden, um die Nutzung der übergreifenden Repositories aus E-Inf-09 zu etablieren, die Konsistenz der Spezifikation zu gewährleiten und die Verwaltung der Use Cases zu vereinfachen. Dies bedingt natürlich, dass die angesprochenen Empfehlungen im Repository technisch umgesetzt sind.
- Security-by-Design-Empfehlung E-Org-04:
  Einführung und Nutzung eines **geeigneten Änderungsmanagements**, das für Nachvollziehbarkeit und Konsistenz sorgt, z. B. durch die Überwachung von Abhängigkeiten: „Wenn an dieser Stelle etwas geändert wird, muss an folgender Stelle auch dies geändert werden.“. Unterstützt wird dies auch durch Umsetzung von E-Inf-01 sowie E-Inf-04 bis -07.
- Security-by-Design-Empfehlung E-Org-05:
  Nachträgliche grundlegende Änderungen sind zu vermeiden. Erste Abgleiche mit den erforderlichen Beschreibungen aus ISMS-Perspektive sollten möglichst früh erfolgen, da nachträgliche Änderungen wegen komplexer, UC-übergreifender Abhängigkeiten leicht Folgefehler bewirken und zu erheblichen Zusatzaufwänden führen können. Kleine Anpassungen, die keine oder kaum Auswirkungen auf andere Use Cases oder die aufbauenden Analysen haben, sind hiervon ausgenommen, sollten aber E-Org-02 berücksichtigen.

4.5.4 Zusammenfassung der Empfehlungen

Im Folgenden sind die Empfehlungen nochmals in Kurzform dargestellt, letztlich sollen die meisten einer höheren Detaillierung und einer höheren UC-übergreifenden Konsistenz der Inhalte dienen:

E-Dok-01	Alle für ein ISMS relevanten Assets und Assettypen aufnehmen
E-Dok-02	Abhängigkeiten und Beziehungen zwischen Assets möglichst vollständig beschreiben
E-Dok-03	Alle Rollen / Akteure und ihre Zuständigkeiten so vollständig wie möglich beschreiben
E-Inf-01	Verwendung eindeutiger, leicht ersichtlicher Identifikatoren
E-Inf-02	Information über Verwendung personenbezogener Informationen oder andere Inhalte mit erhöhtem Schutzbedarf ergänzen
E-Inf-03	Explizite Darstellung aller getroffenen Annahmen und Voraussetzungen
E-Inf-04:	Verwendung von Indentifikatoren für Annahmen und Kontextinformationen
E-Inf-05:	Verknüpfung von Szenarien mit Zielen
E-Inf-06:	Verknüpfung von Szenarien mit Alternativszenarien
E-Inf-07:	Verknüpfung von Anforderungen mit Zielen
E-Inf-08	Verwendung eines UC-übergreifenden Anforderungs-Katalogs
E-Inf-09	Verwendung eines UC-übergreifenden Asset-Repositories
E-Inf-10:	Erstellung eines Assurance Cases
E-Org-01	Einsatz einer UC-übergreifenden Redaktion
E-Org-02	Inkrementelle UC-Erfassung in mehrere Phasen
E-Org-03	Nutzung eines Use Case Repositories von Beginn an
E-Org-04	Einführung und Nutzung eines geeigneten Änderungsmanagements
E-Org-05	Nachträgliche grundlegende Änderungen vermeiden

Tabelle 9: Tabellarische Zusammenfassung der Empfehlungen

5 Übergreifende Listen und Kataloge

Zur vollständigen Beschreibung der beteiligten Akteure und Assets ist es hilfreich, vorhandene übergreifende Listen und Kataloge im UC-Template zu nutzen. Dies kann eine nötige Detailtiefe sowie ein gemeinsames Vokabular und Verständnis fördern. Zusätzlich können entsprechende Vorlagen / Vorgaben das Erstellen einer etablierten Sicherheitslösung unterstützen. Deshalb werden im Folgenden initial übergreifende Listen und Kataloge vorgestellt, die als Ausgangspunkt für eine zukünftige Nutzung der Use-Case-Methodik für das Security-by-Design dienen können.

5.1 Relevante Asset-Typen

Die IT-Grundschutz-Modellierung basiert auf einer genauen Inventarisierung des zu schützenden IT-Systems in Bezug auf Standorte, Infrastruktur, Hardware, Software und Geschäftsprozesse. Die Use-Case-Beschreibung muss entsprechende Angaben enthalten, um diesen Modellierungsschritt nahtlos zu unterstützen.

Bei der Strukturanalyse eines Informationsverbundes nach der Methodik des IT-Grundschutzes zur Einführung eines ISMS werden die Assets in mehrere Gruppen (Assets-Typen) aufgeteilt, die sich hinsichtlich ihrer Eigenschaften, relevanter Gefährdungen und Risiken sowie hinsichtlich der zu erfüllenden Sicherheitsanforderungen grundsätzlich unterscheiden. Diese Typisierung, die im Hinblick auf die Eigenschaften eines Assets bereits Wesentliches aussagt, sollte auch bei der Einteilung und Darstellung der Assets in den Use Cases verwendet werden. Falls das nicht direkt möglich ist, sollte zumindest eine vergleichbare Typisierung strukturell unterstützt werden, damit alle Assets nach Typen unterscheidbar und möglichst typgerecht erfasst und beschrieben werden können, was die Nutzung der Use Cases als Grundlage für ein ISMS sehr erleichtert.

Dabei geht es entsprechend der Methodik des IT-Grundschutzes um folgende Asset-Typen:

- **Geschäftsprozesse**
  Geschäftsprozesse lassen sich als UC definieren und modellieren.
- **Informationen**
  Informationen lassen sich als Informationsobjekte in den UC definieren und inhaltlich beschreiben.
- **Anwendungen**
  Anwendungen lassen sich analog zu den Geschäftsprozessen als einzelne UC Szenarien definieren und modellieren.
- **IT-Systeme:** Server, Clients
  Hier bietet die UC-Struktur gemäß IEC 62559 keine direkte Abbildung. Ein Workaround wäre eine Modellierung auf Basis von Anwendungen, die ja typischerweise auf einzelnen IT-Systemen ausgeführt werden. Im Konzept der UC-Szenarien könnte das Datenfeld „Primary Actor“ dafür verwendet werden. Alle IT-Systeme selbst müssten dann natürlich als Akteure modelliert worden sein.

- **Netze / Kommunikation**: Netze, Netzkomponenten, Kommunikationsverbindungen
  Auch hier bietet die UC-Struktur keine direkte Abbildung. Ein Workaround ist die Modellierung als Requirement eines Informationsobjektes.
- **Infrastruktur: Gebäude, Räume, Gelände**
  Hier bietet die UC-Struktur keine direkte Abbildung. Ein Workaround ist die Modellierung als UC-spezifische Eigenschaften der Akteure. Dabei ist aber auf einheitliche Namensgebung der Infrastrukturtypisierung zu achten.

5.2 ENTSO-e Harmonized Electricity Role Model

Als initiale Akteursliste kann auf das „ENTSO-E Harmonized Electricity Role Model“ zurückgegriffen werden, das für alle Rollen und Domänen, die im Elektrizitätsmarkt verbreitet sind, jeweils einen Begriff benennt und beschreibt. Die aktuellste Version des Modells ist von 2019 und über die Webseite der ENTSO-E frei verfügbar[13]. Es wird dabei zwischen Rollen, Domänen, Ressourcen, Accounts und CIM-Objekten unterschieden. Insgesamt sind allein bei den Rollen über 40 Instanzen beschrieben. Leider sind die Bezeichnungen und Beschreibungen alle auf Englisch, in der nachfolgenden Tabelle 10 sind daher nur die Rollenbezeichnungen auf Englisch und von den Autoren ins Deutsche übersetzt aufgeführt, soweit es deutsche Entsprechungen gab, auf die Übersetzung der Rollenbeschreibungen wurde an diesen Stellen verzichtet.

Typ	Rollenbezeichnung ENTSO-E	zugehörige deutsche Rolle
Rolle	Balance Responsible Party	Bilanzkreisverantwortlicher
Rolle	Balance Supplier	Lieferant
Rolle	Balancing Service Provider	Bereitsteller für Regelenergie
Rolle	Billing Agent	Rechnungssteller
Rolle	Capacity Trader	Kapazitäts Händler
Rolle	Consumer	Letztverbraucher
Rolle	Consumption Responsible Party	Bilanzkreisverantwortlicher (Verbrauch)
Rolle	Consent Administrator	*Keine deutsche Entsprechung*
Rolle	Coordinated Capacity Calculator	*Keine deutsche Entsprechung*
Rolle	Coordination Centre Operator	Koordinationsstellenbetreiber
Rolle	Data Provider	Datenbereitsteller
Rolle	Energy Service Company (ESCO)	Energiedienstleistungsunternehmen
Rolle	Grid Access Provider	Netzbetreiber

[13] https://www.entsoe.eu/digital/cim/role-models/ https://eepublicdownloads.blob.core.windows.net/public-cdn-container/clean-documents/EDI/Library/HRM/Harmonised_Role_Model_2019-01.pdf (Abruf 15.04.2020)

Typ	Rollenbezeichnung ENTSO-E	zugehörige deutsche Rolle
Rolle	Imbalance Settlement Responsible	Bilanzkoordinator/Martkgebietsverantwortlicher
Rolle	Interconnection Trade Responsible	Bilanzkreisverantwortlicher (interconnection trade)
Rolle	LFC Operator	Übertragungsnetzbetreiber
Rolle	Market Information Aggregator	Aggregator Marktinformationen
Rolle	Market Operator	Marktbetreiber
Rolle	Merit Order List Responsible	Verantwortlicher Merit-Order-Liste
Rolle	Meter Administrator	Messdienstleister
Rolle	Meter Operator	Messstellenbetreiber
Rolle	Metered Data Aggregator	Messdatenaggregator
Rolle	Metered Data Collector	Messdienstleister
Rolle	Metered Data Responsible	Messdienstleister
Rolle	Metering Point Administrator	Netzbetreiber
Rolle	Nominated Electricity Market Operator	Energiemarktbetreiber
Rolle	Nomination Validator	Validierer
Rolle	Party Connected to the Grid	Netzanschlussnehmer
Rolle	Producer	Erzeuger
Rolle	Production Responsible Party	Bilanzkreisverantwortlicher (Erzeuger)
Rolle	Reconciliation Accountable	Lieferant
Rolle	Reconciliation Responsible	Netzbetreiber
Rolle	Reserve Allocator	Reserve-Koordinator
Rolle	Resource Aggregator	Aggregator
Rolle	Resource Provider	Einsatzverantwortlicher
Rolle	Scheduling Agent	Fahrplankoordinator
Rolle	Scheduling Area Responsible	Einsatzplanungsverantwortlicher
Rolle	System Operator	Übertragungsnetzbetreiber
Rolle	Trade Responsible Party	Bilanzkreisverantwortlicher (Handel)
Rolle	Trader	Händler
Rolle	Transmission Capacity Allocator	Übertragungskapazitätskoordinator

Tabelle 10: Rollen aus dem ENTSO-E Harmonized Electricity Role Model

Diese Liste beinhaltet lediglich die Rollen aus dem ENTSO-E Role Model, es werden dort auch Ressourcen genannt, unter die beispielsweise eine Erzeugungsanlage fällt, oder Domänen

wie zum Beispiel ein Messpunkt. Des Weiteren fallen im deutschen Bereich meist mehrere Rollen auf einen einzelnen Akteur, wie beispielsweise den Netzbetreiber. Dennoch eignet sich diese Liste gut als Ausgangspunkt für die Analyse, gerade auch, da sie mit der Branche harmonisiert ist.

5.3 Erstellung von Informationsobjektkatalogen

Der Inhalt dieses Kapitels findet sich auch im gleichnamigen Kapitel 3.8 im Ergebnisdokument AS 12.2.22 „Gap-Analyse“ [8].

Die Use-Case-Methodik gemäß IEC 62559 besteht in ihrem Kern aus der Dokumentation der zeitlichen Abfolge von Informationsflüssen zwischen den am Use Case beteiligten Akteuren. Analog zu den Akteuren bedarf es auch hier einer Use-Case-übergreifenden Vereinheitlichung der Terminologie, um auch die Informationsschnittstellen zwischen verschiedenen Use Cases richtig identifizieren zu können.

Idealerweise sollten daher Informationsobjektkataloge der ausgetauschten Objekte erstellt werden, bevor mit der Erstellung der Use Cases begonnen wird. Speziell bei der werkzeugbasierten Use-Case-Erstellung werden auf diese Weise Terminologieprobleme bei der (semantischen) Benennung von Informationsobjekten vermieden.

Es ist allerdings sehr schwierig, im Vorhinein alle Datenflüsse und ausgetauschten Informationen zu kennen, um einen umfassenden Informationsobjektkatalog aufzubauen. Da die meisten Schnittstellen für Informationsflüsse aber auf offenen, internationalen Standards basieren, könnte hier über die Standardisierung Abhilfe geschaffen werden. Viele internationale Kommunikationsstandards beinhalten mittlerweile auch eine Datenmodellbeschreibung für die übertragenen Informationen, wie z. B. die IEC 61850 oder IEC 61968/70 (CIM). Die in diesen Standards verwendete Datenstruktur und Terminologie könnte als Basis für einen Informationsobjektkatalog verwendet werden.

Allerdings sind die bestehenden Standards nicht überschneidungsfrei und es gibt oftmals, wie etwa bei den Standards IEC 61850 oder IEC 61970, keine Abbildungsvorschriften für den überlappenden Bereich der Standardfamilien. Hier ist die Standardisierung gefordert, entsprechende Ontologien zu schaffen, um eine eineindeutige Abbildung zwischen Informationsobjekten mit gleicher Bedeutung und unterschiedlicher Terminologie zu schaffen.

Darüber hinaus sollten Informationsobjektkataloge auch unterschiedliche Detailierungsebenen unterstützen und dabei auch die Zusammenhänge zwischen den verschiedenen Detailierungsstufen abbilden können. So wurden im Projekt enera für die Schutzbedarfsanalyse die detaillierten Informationsobjekte aus den ausgewerteten Use Cases auf ein „High-Level-Datenmodel“ abgebildet, für dessen Ausprägungen dann die initiale Schutzbedarfsfeststellung erfolgte. Neben den Abbildungsvorschriften für gleichbedeutende Informationsobjektbezeichnungen zwischen verschiedenen Standards bedarf es der Einführung einer Art Hierarchie (Taxonomie), die angibt, ob es zu einem Informationsobjektbezeichner einen übergeordneten Sammelbegriff gibt. Ein Beispiel hierfür ist: Die Informationsobjektbezeichnungen „Straßenname“, „Hausnummer“, „Postleitzahl“, „Stadt“, „Bundesland“ können unter dem Begriff „Adressdaten“

subsummiert werden. Solch eine Begriffshierarchie könnte von der Standardisierung im Rahmen eines durchgängigen Terminologiemanagements implementiert werden.

Weiterhin besteht die Möglichkeit, für High-Level-Informationsobjekte Vorschläge für die Schutzbedarfsfeststellung für die einzelnen Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit oder auch in Bezug auf Datenschutz als eine Art Blaupause zu hinterlegen, so dass bei zukünftigen Sicherheitsanalysen ein schnelleres und vereinfachtes Vorgehen möglich ist. Beispielsweise könnte eine vorgegebene Taxonomie bereits Hinweise enthalten, ob es sich bei der bezeichneten Informationsobjektklasse um personenbezogene oder gar um besondere personenenbezogene Daten handelt, für die dann entsprechende Mindeststandards in Bezug auf Vertraulichkeit gelten. Außerdem führt dieses Vorgehen aufgrund der Vergleichsmöglichkeit durch Vorschläge ebenfalls zu einem etablierteren Sicherheitskonzept.

Die CEN-CENELEC hat das Thema einer domänenübergreifenden Ontologie mit einem Workshop aufgegriffen, um mit Experten darüber zu diskutieren, wie diese Aufgabenstellung angegangen werden kann. Im Nachgang zu den CEN-CENELEC Mapping Ontologies Workshop im November 2018, wird dieses Ontology-Arbeit nun innerhalb der CEN-CENELEC Ad-hoc-Gruppe „Energiemanagement Ontologie“ fortgesetzt. Die unter dem Dach von CLC / TC 205 „Home and Building Electronic Systems“ (HBES) eingesetzte Ad-hoc-Gruppe zielt auf die Entwicklung einer gemeinsamen Standard-Ontologie für die bei CEN, CENELEC, ISO und IEC vorhandenen Datenmodellen ab.[14]

5.4 Beispiel für einen Informationsobjektekatalog

Im Rahmen des Projektes enera wurden während der Projektlaufzeit High-Level-Informationsobjekte eingeführt, die bei der Klassifizierung von Informationsobjekten helfen sollten. Diese sind in Tabelle 11 aufgeführt.

Abkürzung	Bezeichnung	Beschreibung
MW_Einzel	Einzelmesswert (Echtzeitnah)	Einzelner Messwert, der von einem Gerät im Netz oder von einer Anlage an ein zentrales System (z.B. SCADA) zyklisch mit geringer Latenzzeit übertragen wird.
MW_Aggregiert	Aggregierter Messwert mehrerer Anlagen (Echtzeitnah)	Messwerte, z. B Schaltzustände, die von mehreren Geräten im Netz oder von mehreren Anlagen an ein zentrales System (z. B. SCADA) spontan mit geringer Latenzzeit übertragen und zu einem Gesamtwert aggregiert wurden.

[14] Siehe auch https://www.cencenelec.eu/News/Publications/Publications/CEN-CENELEC_WP_2020_EN.pdf.

Abkürzung	Bezeichnung	Beschreibung
MW_NetzzustandNS	Netzzustandsdaten aus der Niederspannungsebene	Netzzustandsdaten aus dem Niederspannungsbereich (230 / 400 V)
MW_NetzzustandMS	Netzzustandsdaten aus der Mittelspannungsebene	Netzzustandsdaten aus dem Mittelspannungsbereich (1 - 50 kV)
MW_NetzzustandHS	Netzzustandsdaten aus der Hoch- / Höchstspannungsebene	Netzzustandsdaten aus dem Hoch- und Höchstspannungsbereich (110 bzw. 220 / 380 kV)
MW_Zeitreihe	Zeitreihe von Messwerten	Zeitreihe von Einzelmesswerten die en bloc übertragen oder aus einem Archivsystem abgefragt werden.
MW_AnlagenStatus	Sonstiger Anlagenstatus	Statusinformation über den Funktionszustand des Messwerterfassungs- und -übertragungssystems bzw. einer überwachten Anlage
SMW_Einzel	SM_Einzelmesswert (Echtzeit)	Einzelner Zähler-Messwert, der von einem Smart Meter an ein zentrales System (z. B. MDM) mit geringer Latenzzeit übertragen wird.
SMW_Aggregiert	Aggregierter SM-Messwert (Echtzeit)	Zähler-Messwerte, die von einem Smart Meter an ein zentrales System (z. B. MDM) mit geringer Latenzzeit übertragen und zu einem Gesamtwert aggregiert wurden.
SMW_Zeitreihe	Zeitreihe von SM-Messwerten	Zeitreihe von Zähler-Einzelmesswerten die en bloc übertragen oder aus einem Archivsystem abgefragt werden.
SMW_AnlagenStatus	SM-Anlagenstatus	Statusinformation über den Funktionszustand des Smart Meters bzw. der Smart Meter Kommunikationsinfrastruktur
Strg_Einzelbefehl	Fahrplan oder Einzelbefehl bzw. Steuersignal zum Steuern mehrerer Geräte	Einzelner Befehl oder Fahrplan, der von einem zentralen System (z. B. SCADA) an ein Gerät oder mehrere Geräte (bis 30 kW geschalteter Gesamtleistung) im Netz oder an eine Anlage mit geringer Latenzzeit übertragen wird.
Strg_BroadcastBefehl	Fahrplan oder Broadcast-Steuersignal zum Steuern mehrerer Geräte	Einzelner Befehl oder Fahrplan, der von einem zentralen System (z. B. SCADA) an ein Gerät (bis 100 kW geschalteter

Abkürzung	Bezeichnung	Beschreibung
		Gesamtleistung) im Netz oder an eine Anlage mit geringer Latenzzeit übertragen wird.
Prog_Eingang	Prognoseeingangsdaten	Inputdaten für eine Prognoseapplikation, üblicherweise Messwertreihen, die von anderen Systemen in ein Archiv geschrieben wurden.
Prog_ErgebnisAnlage	Aggregierte und sonst. Prognosen	Prognose für die erwarteten (Energie-) Daten von Anlagen können sowohl Summen- als auch Einzelprognosen sein.
Prog_ErgebnisRegion	Aggregierte und sonst. Prognosen	Prognose für die erwarteten (Energie-) Daten ganzer Regionen können sowohl Summen- als auch Einzelprognosen sein.
FP_Einzel	Einzelfahrplan	Erzeugungs- oder Verbrauchsfahrplan einer einzelnen Anlage, üblicherweise als Zeitreihe beschrieben.
FP_Gruppe	Gruppenfahrplan	Aggregierter Erzeugungs- oder Verbrauchsfahrplan einer Anlagengruppe, üblicherweise als Zeitreihe beschrieben.
FP_BM_Abschalt	Betriebsmittelabschaltplan	Fahrplan für die Abschaltzeiten (z. B. für Wartungsarbeiten) von Betriebsmitteln
Flex_Markt_Anf	Marktanforderung	Ein Gebot oder eine Nachfrage nach Energie (-Flexibilität) an einem Energiemarkt.
Flex_Markt_Inf	Marktinformationen	Ein Überblick über alle aktuell platzierten Gebote oder Nachfragen an einem Energiemarkt
Flex_Markt_Erg	Marktergebnis	Ein durch Abstimmung von Angebot und Nachfrage am Markt abgeschlossenes Energie(-Flexibilitäts-)geschäft
Abr_Energiedaten	Energiedaten	Aggregierte Einspeise / Verbrauchsdaten mit allen Informationen, die für eine Rechnungslegung benötigt werden.
Abr_Rechnungsdaten	Rechnungsdaten	Abrechnungsdaten, die für eine finanzielle Rechnungsbegleichung benötigt werden.

Abkürzung	Bezeichnung	Beschreibung
AM_BMdaten	Betriebsmitteldaten	Technische Betriebsmitteldaten aus dem Datenblatt; Grundlage, um für das Betriebsmittel mathematische Modelle zu erstellen.
AM_Betriebsdaten	Betriebsdaten	Auszeichnung der Betriebszustände eines Betriebsmittels; Grundlage, um zum Beispiel nötige Wartungsmaßnahmen zu bestimmen.
AM_Wartungsdaten	Wartungsdaten	Alle Daten, die für die Planung, Ausführung und Dokumentation von Wartungsmaßnahmen an Betriebsmitteln benötigt werden.
Netz_Topo	Topologiedaten	Daten, die die primärprozesstechnische Konnektivität der Betriebsmittel beschreiben (Strom: elektrisch; Gas: Druck)
Netz_BMdaten	Elektr. Betriebsmitteldaten	Elektrische Betriebsmitteldaten aus dem Datenblatt; Grundlage, um für das Betriebsmittel mathematische Modelle zu erstellen.
Netz_Geodata	Geographiedaten	Daten, welche die geographische Position oder Ausdehnung eines Betriebsmittels beschreiben.
Netz_ZustandDesNetzesNS	Zustand des Niederspannungsnetzes	Der Zustand des Netzes in der Niederspannung wird aus den erfassten Netzzustandsdaten (NS) abgeleitet und zum Beispiel in Form von Ampelbewertungen ausgegeben.
Netz_ZustandDesNetzesMS	Zustand des Mittelspannungsnetzes	Der Zustand des Netzes in der Mittelspannung wird aus den erfassten Netzzustandsdaten (MS) abgeleitet und zum Beispiel in Form von Ampelbewertungen ausgegeben.
Netz_ZustandDesNetzesHS	Zustand des Hoch- / Höchstspannungsnetzes	Der Zustand des Netzes in der Hoch- und Höchstspannung wird aus den erfassten Netzzustandsdaten (HS) abgeleitet und zum Beispiel in Form von Ampelbewertungen ausgegeben.
KD_Tech	Technische Kundendaten	Daten über installierte Anlagen, sowie Konfigurationsdaten für diese Anlagen

Abkürzung	Bezeichnung	Beschreibung
KD_Stammdaten	Kundenstammdaten	Alle Daten, die zu einem Stromkunden/Netzanschlussnehmer gespeichert werden.
KD_Kom	Kundenkommunikationsdaten	Aufzeichnung der Information, die zum Kunden gesendet oder von diesem erhalten wurden.
Misc_NA	Not Applicable	Daten, die nicht in das Schema des HL-Datenmodels passen.

Tabelle 11: In enera verwendete High-Level Informationsobjekte

5.5 Beispiel für einen Anforderungskatalog

Über die Anforderungen (UC-Abschnitt 6 „Requirements“) können diverse Arten von Anforderungen wie beispielsweise an die Latenzzeit für Kommunikation oder die Häufigkeit eines Informationsaustauschs beschrieben werden. Es können hierüber jedoch auch Sicherheitsanforderungen oder nicht-technische Anforderungen – beispielsweise rechtlicher Art (ein Vertrag muss vorliegen etc.) – hinterlegt werden. Das hier gegebene Beispiel beschränkt sich auf Information Security.

Wie in Kapitel 4.3 beschrieben, wurde bei der Schutzbedarfsfeststellung eine Vererbung von Schutzbedarfen der High-Level InfoObjekte über die Informationsobjekte auf die zugehörigen Anwendungssysteme, Infrastruktur und Netze / Kommunikationsverbindungen angewandt. Mit dem Vererbungsprinzip kann eine Einschätzung des Schutzbedarfs bei den ausgetauschten Informationen über die Requirements im UC-Template die Schutzbedarfsfeststellung erheblich unterstützen. Daher kann ein Anforderungskatalog wie folgt aussehen:

Requirements		
Categories ID	**Category name for requirements**	**Category description**
SCHUTZ	Schutzbedarf	Einschätzung der Schadenshöhe bei Verletzung der Grundwerte Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität. Dabei empfiehlt die IT-Grundschutz-Methodik drei Schutzbedarfskategorien: • **normal:** Die Schadensauswirkungen sind begrenzt und überschaubar. • **hoch:** Die Schadensauswirkungen können beträchtlich sein. • **sehr hoch:** Die Schadensauswirkungen können ein existentiell bedrohliches, katastrophales Ausmaß erreichen.
Requirement ID	**Requirement name**	**Requirement description**

SCHUTZ-VERTR-normal	Normale Vertraulichkeit	Einschätzung der Anforderungen an die **Vertraulichkeit** ist **normal**: Die Schadensauswirkungen bei Verletzung der Vertraulichkeit sind begrenzt und überschaubar.
SCHUTZ-VERTR-hoch	Hohe Vertraulichkeit	Einschätzung der Anforderungen an die **Vertraulichkeit** ist **hoch**: Die Schadensauswirkungen bei Verletzung der Vertraulichkeit können beträchtlich sein.
SCHUTZ-VERTR-sehrhoch	Sehr hohe Vertraulichkeit	Einschätzung der Anforderungen an die **Vertraulichkeit** ist **sehr hoch**: Die Schadensauswirkungen bei Verletzung der Vertraulichkeit können ein existentiell bedrohliches, katastrophales Ausmaß erreichen.
SCHUTZ-INTEG-normal	Normale Integrität	Einschätzung der Anforderungen an die **Integrität** ist **normal**: Die Schadensauswirkungen bei Verletzung der Integrität sind begrenzt und überschaubar.
SCHUTZ-INTEG-hoch	Hohe Integrität	Einschätzung der Anforderungen an die **Integrität** ist **hoch**: Die Schadensauswirkungen bei Verletzung der Integrität können beträchtlich sein.
SCHUTZ-INTEG-sehrhoch	Sehr hohe Integrität	Einschätzung der Anforderungen an die **Integrität** ist **sehr hoch**: Die Schadensauswirkungen bei Verletzung der Integrität können ein existentiell bedrohliches, katastrophales Ausmaß erreichen.
SCHUTZ-VERF-normal	Normale Verfügbarkeit	Einschätzung der Anforderungen an die **Verfügbarkeit** ist **normal**: Die Schadensauswirkungen bei Verletzung der Verfügbarkeit sind begrenzt und überschaubar.
SCHUTZ-VERF-hoch	Hohe Verfügbarkeit	Einschätzung der Anforderungen an die **Verfügbarkeit** ist **hoch**: Die Schadensauswirkungen bei Verletzung der Verfügbarkeit können beträchtlich sein.
SCHUTZ-VERF-sehrhoch	Sehr hohe Verfügbarkeit	Einschätzung der Anforderungen an die **Verfügbarkeit** ist **sehr hoch**: Die Schadensauswirkungen bei Verletzung der Verfügbarkeit können ein existentiell bedrohliches, katastrophales Ausmaß erreichen.
SCHUTZ-AUTH-normal	Normale Authentizität	Einschätzung der Anforderungen an die **Authentizität** ist **normal**: Die Schadensauswirkungen bei Verletzung der Authentizität sind begrenzt und überschaubar.
SCHUTZ-AUTH-hoch	Hohe Authentizität	Einschätzung der Anforderungen an die **Authentizität** ist **hoch**: Die Schadensauswirkungen bei Verletzung der Authentizität können beträchtlich sein.
SCHUTZ-AUTH-sehrhoch	Sehr hohe Authentizität	Einschätzung der Anforderungen an die **Authentizität** ist **sehr hoch**: Die Schadensauswirkungen bei Verletzung der Authentizität können ein existentiell bedrohliches, katastrophales Ausmaß erreichen.

Tabelle 12: Beispiel eines Anforderungskatalogs der Kategorie Schutzbedarf

Zur Erläuterung der Grundwerte Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität können im Glossar im UC-Template (UC-Abschnitt 8) die Definitionen des BSI [13] aufgegriffen werden:

Common terms and definitions	
Term	**Definition**
Authentizität	Mit dem Begriff Authentizität wird die Eigenschaft bezeichnet, die gewährleistet, dass ein Kommunikationspartner tatsächlich derjenige ist, der er vorgibt zu sein. Bei authentischen Informationen ist sichergestellt, dass sie von der angegebenen Quelle erstellt wurden. Der Begriff wird nicht nur verwendet, wenn die Identität von Personen geprüft wird, sondern auch bei IT-Komponenten oder Anwendungen.
Integrität	Integrität bezeichnet die Sicherstellung der Korrektheit (Unversehrtheit) von Daten und der korrekten Funktionsweise von Systemen. Wenn der Begriff Integrität auf „Daten“ angewendet wird, drückt er aus, dass die Daten vollständig und unverändert sind. In der Informationstechnik wird er in der Regel aber weiter gefasst und auf „Informationen“ angewendet. Der Begriff „Information“ wird dabei für „Daten“ verwendet, denen je nach Zusammenhang bestimmte Attribute wie z. B. Autor oder Zeitpunkt der Erstellung zugeordnet werden können. Der Verlust der Integrität von Informationen kann daher bedeuten, dass diese unerlaubt verändert, Angaben zum Autor verfälscht oder Zeitangaben zur Erstellung manipuliert wurden.
Verfügbarkeit	Die Verfügbarkeit von Dienstleistungen, Funktionen eines IT-Systems, IT-Anwendungen oder IT-Netzen oder auch von Informationen ist vorhanden, wenn diese von den Anwendern stets wie vorgesehen genutzt werden können.
Vertraulichkeit	Vertraulichkeit ist der Schutz vor unbefugter Preisgabe von Informationen. Vertrauliche Daten und Informationen dürfen ausschließlich Befugten in der zulässigen Weise zugänglich sein.

Tabelle 13: Definition der Grundwerte Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität gemäß BSI IT Grundschutz Glossar [13]

Je nach Anwendungsszenario und je nach vorgesehener Hardware und Software, die zum Einsatz kommen soll, gibt es ein breites Spektrum an potentiell relevanten Sicherheitsanforderungen, das sich an dieser Stelle nicht umfassend darstellen lässt. Generell richten sich die Anforderungen aber nach dem Schutzbedarf der jeweiligen Komponente oder des jeweiligen Prozessschritts, und hier sind vor allem die zu schützenden Sicherheitsgrundwerte relevant. Tabelle 14 zeigt beispielhaft einige grundlegende Sicherheitsgrundwerte, typische Maßnahmen zu deren Gewährleistung und entsprechende Sicherheitsanforderungsklassen.

Sicherheitsgrundwert	**Typische Maßnahmen**	**Anforderungen bzgl. …**
Vertraulichkeit	Zugriffsschutz, Verschlüsselung	Zugriffskontrolle, Kryptografie
Integrität	Zugriffsschutz, Kryptografische Prüfsummen	Zugriffskontrolle, Kryptografie

Sicherheitsgrundwert	Typische Maßnahmen	Anforderungen bzgl. …
Verfügbarkeit	Redundanz, Backups	Hochverfügbarkeitsarchitektur, Datensicherung
Authentizität	Personalisierte Systemkennung und Passwort, signierte Daten, signierter Code	Authentisierung, digitale Signaturen
Nichtabstreitbarkeit	Audit Trail, Unterschriften	Monitoring, Logging, digitale Signaturen
Physische Sicherheit	Zutrittsbeschränkungen, Alarmsystem, Videoüberwachung, Einbruch-hemmende Bauweise, Verplombung	Zugangskontrolle, physische Härtung

Tabelle 14: Sicherheitsgrundwerte und entsprechende Sicherheitsanforderungsklassen

Je nach betroffenen Grundwerten in einem Use Case kann ein Standard-Repertoire an relevanten Anforderungen zusammengestellt und als vorgefertigter Katalog im Use-Case-Managementsystem bereitgestellt werden, um im Projekt eine einheitliche Terminologie und ein einheitliches Verständnis über den Schutzbedarf zu fördern. Im Folgenden verweisen wir auf empfohlene Quellen, aus denen sich entsprechende Anforderungen entnehmen lassen.

5.5.1 BSI Grundschutzkompendium

Eine gute Quelle für Sicherheitsanforderungen ist das Grundschutzkompendium[15] des Bundesamts für Sicherheit in der Informationstechnik (BSI). Es umfasst Systembausteine für die gängigsten Komponenten eines IT-Systems sowie für Standardanwendungen und wichtige Dienste. Insbesondere finden sich auch Bausteine für Industrielle IT (IND), Netze und Kommunikation (NET) und Infrastruktur (INF). Jeder Baustein beinhaltet Sicherheitsanforderungen auf drei verschiedenen Sicherheitsniveaus: Basisanforderungen, Standardanforderungen und Anforderungen bei erhöhtem Schutzbedarf.
Abgesehen von Anforderungen an die IT-Technik bietet das Grundschutzkompendium aber auch Anforderungen and organisatorische Prozesse (Baustein ORP) und an Konzepte und Vorgehensweisen (Baustein CON). In Bezug auf Security-by-Design liefert insbesondere CON eine Fülle von Anregungen, wenn es zum Beispiel um Anforderungen an das Kryptokonzept, an den Datenschutz oder die Datensicherung oder an die Software-Entwicklung geht.

5.5.2 BDEW Whitepaper

Speziell für den Energiesektor fasst auch das Whitepaper „Anforderungen an sichere Steuerungs- und Telekommunikationssysteme“[16] des BDEW die grundlegenden Sicherheitsanforderungen an die die Informations- und Kommunikationstechnik in diesem Bereich zusammen.

[15] Siehe https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/it-grundschutz-kompendium_node.html (Stand: 17.03.2021).
[16] Siehe https://www.bdew.de/service/anwendungshilfen/whitepaper-anforderungen-sichere-steuerungs-telekommunikationssysteme/ (Stand: 17.03.2021).

Das Whitepaper definiert Anforderungen an Einzelkomponenten und für aus diesen Komponenten zusammengesetzte Systeme und Anwendungen. Ergänzend werden auch Sicherheitsanforderungen an Wartungsprozesse, Projektorganisation und Entwicklungsprozesse behandelt. Der Fokus des Dokuments sind die im Rahmen der Beschaffung zu berücksichtigenden Anforderungen an technische Komponenten, Systeme und für die Projektabwicklung relevanten Prozesse. Dies bietet eine domänenspezifische Ergänzung zum BSI Grundschutzkompendium.

6 Use Case-Template: Vorschläge zu Erweiterungen und verbesserter Nutzung

Im Use Case-Template gemäß IEC 62559 wird das Thema Informationssicherheit nicht explizit adressiert. Es können allerdings in UC-Abschnitt 6 bereits Sicherheitsanforderungen benannt werden, die dann in der Beschreibung der einzelnen Szenarioschritte in UC-Abschnitt 4.2 referenziert werden können, siehe auch die in Kapitel 3 dargestellten Tabellen (Tabelle 7 und Tabelle 8). Dies wurde bisher allerdings in der praktischen Umsetzung kaum angewendet. Entsprechend der Empfehlungen aus Kapitel 4 soll das Use Case-Template in der Art erweitert werden, dass Informationssicherheitsaspekte bereits von Beginn an im Entwicklungsprozess mitberücksichtigt werden können (Security-by-Design). Im Folgenden werden die Erweiterungen gemäß der Empfehlungen aus Kapitel 4 in das UC-Template integriert. Dazu werden im Folgenden die betroffenen Template-Abschnitte der Reihe nach erörtert.

6.1 UC-Template Abschnitt 1 (“Description of the use case”)

Gemäß E-Org-02 wird eine Unterteilung der UC-Erfassung in mehrere Phasen empfohlen. Die erste Phase sollte dabei maximal die allgemeine Beschreibung des Use Cases im Abschnitt 1 und erste Diagramme im Abschnitt 2 des UC-Templates beinhalten. Eine noch stärkere Untergliederung ist möglich.

1.2 Version management

Version management				
Version No.	***Date***	***Name of author(s)***	***Changes***	***Approval status***

Tabelle 15: Abschnitt 1.2 des UC-Templates: Version management

Gemäß E-Inf-03 sollten alle getroffenen Annahmen und Voraussetzungen dokumentiert werden. Dies ist natürlich nicht ab der ersten Version des Use Cases der Fall. Daher sollte beim *Approval status* in Abschnitt 1.2 („Version management“) vermerkt werden, wie weit fortgeschritten der Use Case – auch in Hinblick auf die Security-Aspekte – dokumentiert ist, siehe Tabelle 15.

1.6 Use case conditions

Use case conditions
Assumptions
Prerequisites

Tabelle 16: Abschnitt 1.6 des UC-Templates: Use case conditions

In Abschnitt 1.6 („Use case conditions“) sind alle getroffenen Annahmen und Voraussetzungen darzustellen, und mit einem Identifikator zu versehen. Siehe Empfehlung E-Inf-03 und E-Inf-04 und auch Tabelle 16.

1.8 General remarks

General remarks

Tabelle 17: Abschnitt 1.8 des UC-Templates: General remarks

In Abschnitt 1.8 („General remarks“) kann vermerkt werden, welche Security-Aspekte bereits berücksichtigt wurden, siehe Tabelle 17. Hier empfiehlt es sich auch, eine Unterscheidung zwischen dokumentierten und bereits umgesetzten Sicherheitsmaßnahmen vorzunehmen, insbesondere bei prototypischen Use Cases.

6.2 UC-Template Abschnitt 2 (“Diagrams of use case”)

Diagram(s) of use case

Tabelle 18: Abschnitt 2 des UC-Templates: Diagram of use case

Abschnitt 2 des UC-Templates beinhaltet ein einfaches Feld für zugehörige Diagramme, siehe Tabelle 18. Die Diagramme zum Use Case können generell sehr vielfältig sein. Zur Prüfung auf Vollständigkeit (E-Dok-02) der beteiligten Akteure und der ausgetauschten Informationen in den Szenarioschritten können Sequenzdiagramme herangezogen werden, die automatisch aus den Szenarien im Use Case erstellt werden. Die automatisierte Erstellung von Sequenzdiagrammen ist bei der Verwendung eines Use Case Repositories (E-Org-03) möglich. Use-Case-Diagramme bieten zusätzlich einen ersten Überblick über Systemgrenzen, Akteure und vorhandene Use Cases mit ihren Beziehungen untereinander.

6.3 UC-Template Abschnitt 3 (“Technical details“)

Gemäß E-Org-02 wird empfohlen, diesen Teil des Use Case Templates erst nach Konsolidierung der Informationen des ersten Template-Abschnitts auszufüllen. Die zweite Phase kann dabei die technischen Details, wie in diesem dritten Abschnitt, siehe Tabelle 19, sowie die Übersicht der Szenarien im Abschnitt 4.1 des Templates umfassen.

3.1 Actors

Actors			
Grouping		Group description	
Actor name	Actor type	Actor description	Further information specific to this use case

Tabelle 19: Abschnitt 3.1 des UC-Templates: Actors

Hier sollten alle aus Sicht eines ISMS relevanten Akteure inkl. ihrer Zuständigkeiten aufgenommen und so vollständig wie möglich beschrieben werden, siehe Empfehlung E-Inf-01 und E-Inf-03. Eine Ausnahme bilden die Assets „Informationen“ bzw. Informationsobjekte: Hierfür hat das Use Case-Template einen eigenen Abschnitt.

Gemäß E-Inf-01 wird empfohlen, eine Spalte für die ID des Akteurs zu ergänzen. Des weiteren wurde zur Zuordnung des Akteurs zu einem Akteur aus dem Asset-Repositories gemäß E-Inf-09 eine weitere Spalte im Anpassungsvorschlag ergänzt und für die möglichst vollständige Beschreibung eine Spalte für den Standort, siehe Tabelle 20.

Actors						
Grouping			*Group Description*			
Actor ID	*Actor Name*	***Actor classification***	*Actor type*	***Actor location***	*Actor description*	*Further information specific to this use case*

Tabelle 20: Erweiterter Abschnitt 3.2 des UC-Templates: Actors

6.4 UC-Template Abschnitt 4 ("Step by step analysis of use case")

4.1 Overview of scenarios

Scenario conditions						
No.	***Scenario name***	***Scenario description***	***Primary actor***	***Triggering event***	***Pre-condition***	***Post-condition***

Tabelle 21: Abschnitt 4 des UC-Templates: Overview of scenarios

Gemäß E-Inf-03 sollten im Abschnitt 4 des UC-Templates insbesondere unter „Triggering Event" und „Precondition" alle getroffenen Annahmen und Voraussetzungen explizit dargestellt werden, siehe Tabelle 21, zum Beispiel Annahmen über Sicherheitsgarantien, von denen das Szenario ausgeht. Diese können auf den Identifikator der Annahmen verweisen (siehe E-Inf-04). Auch eine Zuordnung des Szenarios zu Zielen des Use Cases sollte erfolgen (siehe E-Inf-05).

4.2 Steps – Scenarios

Scenario								
Scenario name :								
Step No.	***Event***	***Name of process/ activity***	***Description of process/ activity***	***Service***	***Information producer (actor)***	***Information receiver (actor)***	***Information exchanged (IDs)***	***Requirements R-ID***

Tabelle 22: Abschnitt 4.2 des UC-Templates: Steps - Scenarios

Gemäß E-Dok-02 sollten in den Szenarien die Abhängigkeiten und Beziehungen zwischen den Assets möglichst vollständig beschrieben werden. Hierzu kann auch eine Prüfung der automatisiert aus den Szenarien erstellten Sequenzdiagrammen beitragen.

Über die Nutzung eines Use Case Management Repositories gemäß E-Org-03 kann hier darüber hinaus sichergestellt werden, dass in den Spalten „Information Producer“ und „Information Receiver“ nur Akteure aus der Akteursliste im Abschnitt 3.1 des Templates verwendet werden, siehe Tabelle 22. Dies gilt ebenso für die Synchronisation der „Information Exchanged“ aus Abschnitt 5 des Templates und mit den „Requirements“ im Abschnitt 6, siehe Tabelle 23.

6.5 UC-Template Abschnitt 5 (“Information exchanged“)

Information Exchanged			
Information exchanged ID	***Name of information exchanged***	***Description of information exchanged***	***Requirements IDs***

Tabelle 23: Abschnitt 5 des UC-Templates: Information exchanged

Auch in Abschnitt 5 des UC-Templates sollten gemäß den Dokumentationsempfehlungen alle relevanten Informationen aufgeführt werden. Insbesondere über die „Requirements“ können weitere Sicherheitsanforderungen dokumentiert werden, wie etwa Schutzbedarfe und der Schutz personenbezogener Daten. Zur Verwendung des Informationsobjektkatalogs wird empfohlen, eine weitere Spalte zur Zuordnung des Informationsobjekts zum betreffenden Katalogeintrag einzuführen.

Des Weiteren sollte die UC-übergreifende Redaktion gemäß Empfehlung E-Org-01 sicherstellen, dass alle Anforderungen – insbesondere hinsichtlich Schutzbedarf und bereits angenommener Sicherheitsmaßnahmen wie beispielsweise Verschlüsselung – dokumentiert werden. Für den Schutzbedarf wird empfohlen, eine weitere Spalte einzuführen, bei der die Begründung für eine Anforderung an eine Information angegeben werden kann. Dies ist insbesondere für die Einschätzung der Schutzbedarfe erwünscht, kann aber generell auch bei anderen Anforderungen angewandt werden. Die angenommenen und damit bereits vorgesehenen Sicherheitsmaßnahmen sollen ebenfalls über die Anforderungen dokumentiert werden, wobei der Anforderungskatalog helfen kann, Anforderungen systematisch und in einheitlicher Terminologie zu erfassen, siehe Tabelle 24.

Information Exchanged					
Information exchanged ID	*Name of information exchanged*	***Classification of Information exchanged***	*Description of information exchanged*	*Requirements IDs*	***Reason for Requirement***

Tabelle 24: Erweiterter Abschnitt 5 des UC-Templates: Information exchanged

6.6 UC-Template Abschnitt 6 ("Requirements (optional)")

Requirements (optional)		
Categories ID	***Category name for requirements***	***Category description***
Requirement ID	***Requirement name***	***Requirement description***

Tabelle 25: Abschnitt 6 des UC-Templates: Requirements (optional)

In Abschnitt 6 des UC-Templates ist zu erwähnen, dass es mehrere Kategorien an Anforderungen geben kann und soll. Daher sollte die oben stehende Tabelle 25 mehrfach für verschiedene Anforderungskategorien im Use Case-Template verwendet werden. Eine Anforderungskategorie wären dabei die Sicherheitsanforderungen aus Kapitel 5.5. Es sollten gemäß Empfehlung E-Inf-03 alle Voraussetzungen explizit dargestellt werden.

7 Zusammenfassung der Empfehlungen und Anpassungen

Dieses Kapitel fasst abschließend noch einmal zusammen, auf welche Bereiche des Use-Case-Templates sich die Empfehlungen aus Abschnitt 4.5 auswirken und an welchen Stellen das Template konkret angepasst wurde. Konkrete Anpassungen wurden wie folgt vorgenommen:

- In UC-Template-Abschnitt 3.1 bei den Akteuren wurden drei Spalten ergänzt: für die Akteurs-ID, für die Zuordnung des Akteurs und für seinen Standort (vgl. Tabelle 26).

Actors						
Grouping			*Group Description*			
Actor ID	*Actor Name*	***Actor classification***	*Actor type*	***Actor location***	*Actor description*	*Further information specific to this use case*

Tabelle 26: Anpassungen Abschnitt 3.1 – Actors

- In UC-Template-Abschnitt 5 wurden zwei Spalten bei den ausgetauschten Informationen für die Klassifizierung der ausgetauschten Informationen und für die Bewertung des Schutzbedarfs ergänzt (vgl. Tabelle 27).

Information Exchanged					
Information exchanged ID	*Name of information exchanged*	***Classification of Information exchanged***	*Description of information exchanged*	*Requirements IDs*	***Reason for Requirement***

Tabelle 27: Anpassungen Abschnitt 5 – Information Exchanged

Tabelle 28 fasst darüber hinaus alle durch die Empfehlungen betroffenen Abschnitte des Use-Case-Templates nochmal zusammen.

Nr.	Empfehlung	Betroffene Abschnitte im Use Case-Template
E-Dok-01	Alle für ein ISMS relevanten Assets und Assettypen aufnehmen.	3.1 Actors
E-Dok-02	Abhängigkeiten und Beziehungen zwischen Assets möglichst vollständig beschreiben.	4 Step by step analysis of use case

Nr.	Empfehlung	Betroffene Abschnitte im Use Case-Template
E-Dok-03	Alle Rollen / Akteure und ihre Zuständigkeiten so vollständig wie möglich beschreiben.	3.1 Actors 4 Step by step analysis of use case
E-Inf-01	Verwendung eindeutiger, leicht ersichtlicher Identifikatoren	3.1 Actors 4 Step by step analysis of use case 5 Information exchanged 6 Requirements
E-Inf-02	Information über Verwendung personenbezogener Informationen oder andere Inhalte mit erhöhtem Schutzbedarf	4.2 Steps-Scenarios 6 Requirements
E-Inf-03	Explizite Darstellung aller getroffenen Annahmen und Voraussetzungen	1.6 Use case conditions 6 Requirements
E-Inf-04	Verwendung von Identifikatoren für Annahmen und Kontextinformationen	1.6 Use case conditions
E-Inf-05	Verknüpfung von Szenarien mit Zielen	4.1 Overview of scenarios
E-Inf-06	Verknüpfung von Szenarien mit Alternativszenarien	4.2 Steps-Scenarios
E-Inf-07	Verknüpfung von Anforderungen mit Zielen	6 Requirements
E-Inf-08	Verwendung eines UC-übergreifenden Anforderungs-Katalogs	4.2 Steps-Scenarios 6 Requirements
E-Inf-09	Verwendung eines UC-übergreifenden Asset-Repositories	3.1 Actors 4 Step by step analysis of use case
E-Inf-10	Erstellung eines Assurance Cases	Der Assurance Case wird parallel zum Use Case erstellt, verweist auf die jeweiligen Elemente im Use-Case-Template und stellt ihre Beziehung dar. Des Weiteren können dort auch organisatorische Schritte hinterlegt werden.
E-Org-01	Einsatz einer UC-übergreifenden Redaktion	Die organisatorischen Empfehlungen betreffen die Bearbeitung von Use Cases im Allgemeinen, daher werden sie keinen konkreten Abschnitten im Template zugeordnet. Es ist jedoch zu erwähnen, dass die Nutzung eines Repositories von Beginn an gerade
E-Org-02	Gliederung der UC-Erfassung in mehrere Phasen Vorgeschlagene Phasen: A. Beschreibung des Use Cases im Abschnitt 1 und erste Diagramme im Abschnitt 2 des UC-Templates	

Nr.	Empfehlung	Betroffene Abschnitte im Use Case-Template
	B. Beschreibung der technischen Details im Abschnitt 3 und Übersicht der Szenarien im Abschnitt 4.1 des Templates C. Ausführung der Szenarien in Abschnitt 4.2 des Templates inkl. zugehörigen Informationsobjekten und Anforderungen in den Abschnitten 5 und 6	bei der konsistenten Verwendung von IDs und der Verwendung von übergreifenden Katalogen technisch unterstützt und damit automatisch erzwingen kann.
E-Org-03	Nutzung eines Use Case Repositories von Beginn an. Umsetzungsempfehlung: Implementierung der Kataloge aus Kapitel 5 übergreifend für alle Use Cases; einzeln pro Use Case ein Verweis auf Element aus Katalog und im Use Case eigene, UC-spezifische Instantiierung und Ergänzung.	
E-Org-04	Einführung und Nutzung eines geeigneten Änderungsmanagements	
E-Org-05	Nachträgliche grundlegende Änderungen vermeiden	

Tabelle 28: Auswirkungen der Empfehlungen auf Abschnitte des Use Case-Templates

Bezugsdokumente

Nr.	Bezeichnung	Metadaten	Inhalt	Link / Ablageort / Datei
1	**Anleitung zum Ausfüllen des IEC 62559 Use Case-Templates**	Christina Delfs, Christian Dänekas, Version 2 12.08.2015	Anleitung für Use Case Erstellung im Use Case Management Repository UCMR	Internes Dokument OFFIS
2	**Ergebnisdokument AS 12.2.7**		„Strukturanalyse und Inventarisierung“	enera Sharepoint: 20181221_Ergebnisdokument AS12.2.7_Strukturanalyse_Inventarisierung_V1.00.docx
3	**Ergebnisdokument AS 12.2.8**		„Schutzbedarfsfeststellung“	enera Sharepoint: 20190205_AS12.2.8_Schutzbedarfsfeststellung_V1.00.docx
4	**Ergebnisdokument AS 12.2.9 und AS 12.2.10**		„Schwachstellen- Bedrohungs- und Risikoanalyse“ und „Risikobehandlung“	enera Sharepoint: 20190801_AS12.2.9u10_Schwachstellen-Bedrohungs-Risikoanalyse_und Risikobehandlung_V1.00.docx
5	**Notwendige Ergänzungen und Konkretisierungen der UC in Scope 07**	Fabian Karl, Tobias Richter (PPC), Version 2.3 05.06.2018	„AS 12.2.7 – Strukturanalyse und Schutzbedarfsfeststellung | Scope 07 – Messen und Steuern via SMGW | Notwendige Ergänzungen und Konkretisierungen der Use Cases“	Enera Sharepoint: 2018_06_05_Strukturanalyse_Konkretisierung_der_UC_in_Scope_07_v2_3.pptx
6	**Vorschläge zur Anpassung der UC in Scope 07**	Fabian Karl, Tobias Richter (PPC), Version 2.3 05.06.2018	„Vorschläge zur Anpassung der Use-Cases für eine Konkretisierung der Strukturanalyse in Scope 07“	Enera Sharepoint: 2018-05-18_Ergaenzungen_der_UC_in_Scope_07_v2.docx
7	**Ergebnisdokument AS 12.2.4**		„Governance, Compliance und Datenschutz: Erhebungen, Strukturen und Management“	Enera Sharepoint: 2018-12-07_AS12.2.4_Governance, Compliance und Datenschutz_V1.11.docx
8	**Ergebnisdokument AS 12.2.22**		„Gap-Analyse“	Enera Sharepoint: Ergebnisdokument AS 12.2.22.docx

Nr.	Bezeichnung	Metadaten	Inhalt	Link / Ablageort / Datei
9	**Entwicklung eines Transformationsansatzes zur Integration von Datenschutz und IT-Sicherheit in die Planungsprozesse komplexer Systeme**	Lukas Engel, Masterarbeit, 2018, FAU Erlangen-Nürnberg.	Transformationsansatz zur Integration von Informationssicherheit am Beispiel Smart Grid	*Own Cloud unter: /Enera/AP12/AS 12.2.07 – Strukturanalyse und Inventarisierung/Masterarbeit_Lukas Engel.pdf*
10	**Use Case methodology: a progress report**	Clausen, M., Apel, R., Dorchain, M., Postina, M., & Uslar, M. (2018). Energy Informatics, 1(1), 19.	Erfahrungsbericht der Use Case Erfassung aus enera	*https://link.springer.com/article/10.1186/s42162-018-0036-0*
11	**Buch zum Qualitätsmanagement: Definition der 10er-Regel**		Pfeifer, Tilo: Qualitätsmanagement – Strategien, Methoden, Techniken, 2.,vollst. überarb. und erw. Aufl. München: Hanser, 1996, S. 11.	
12	**Rollenmodell für die Marktkommunikation**		BDEW Bundesverband der Energie- und Wasserwirtschaft e.V., Rollenmodell für die Marktkommunikation im deutschen Energiemarkt, Anwendungshilfe, BDEW, 2016.	*https://www.bdew.de/service/anwendungshilfen/rollenmodell-fuer-die-marktkommunikation-im-deutschen-energiemarkt/*
13	**Glossar IT Grundschutz**		Begriffsdefinitionen vom BSI für den IT Grundschutz	*https://www.bsi.bund.de/DE/Themen/IT-Grundschutz/ITGrundschutzKompendium/vorkapitel/Glossar_.html*
14	Ergebnisdokument AS 12.2.25	Denis Uecker, Reinhard Schwarz (Fraunhofer IESE), Version 1.2, 03.02.2020	Assurance Cases als Leitfaden für die Use-Case-Erhebung	*Own Cloud unter: /Enera/AP12/AS 12.2_IESE/2020-02-03_Assurance Cases als Leitfaden für die Use Case Erhebung_v1.2.pdf*

Abbildungsverzeichnis

Abbildung 1: Phasen der Use Case Bearbeitung (Quelle: [10]) 11
Abbildung 2: Scope-Einteilung und Use Case Akteure verortet im SGAM 13
Abbildung 3: Wechselwirkung zwischen Use Cases und generischem ISMS 14
Abbildung 4: PDCA-Zyklus angelehnt an die ISO/IEC 27001 aus der Masterarbeit zur Thematik [9] 14
Abbildung 5: Vererbung des Schutzbedarfes - Schematische Darstellung 24
Abbildung 6: SGAM Würfel in der 3D Visualisierung 60
Abbildung 7: Übersicht der ausgetauschten Informationen 61
Abbildung 8: Sequenzdiagramm – Use Case mit MS Word® Template erfassen 62
Abbildung 9: Netzplan des Virtuellen Kraftwerks 74

Tabellenverzeichnis

Tabelle 1: Zuordnung von Bestandteilen des IT-Grundschutzprofils im UC-Template 17
Tabelle 2: Abschnitt 4.2 des UC-Templates: Steps-Scenarios 18
Tabelle 3: Abschnitt 5 des UC-Templates: Informations Exchanged 18
Tabelle 4: Abschnitt 6 des UC-Templates: Requirements (optional) 19
Tabelle 5: Abschnitt 3.1 des UC-Templates: Actors 20
Tabelle 6: Abschnitt 8 des UC-Templates: Custom Information (optional) 20
Tabelle 7: Abschnitt 4.2 des UC-Templates: Steps - Scenarios 21
Tabelle 8: Abschnitt 6 des UC-Templates: Requirements (optional) 21
Tabelle 9: Tabellarische Zusammenfassung der Empfehlungen 29
Tabelle 10: Rollen aus dem ENTSO-E Harmonized Electricity Role Model 32
Tabelle 11: In enera verwendete High-Level Informationsobjekte 38
Tabelle 12: Beispiel eines Anforderungskatalogs der Kategorie Schutzbedarf 39
Tabelle 13: Definition der Grundwerte Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität gemäß BSI IT Grundschutz Glossar [13] 40
Tabelle 14: Sicherheitsgrundwerte und entsprechende Sicherheitsanforderungsklassen 41
Tabelle 15: Abschnitt 1.2 des UC-Templates: Version management 43
Tabelle 16: Abschnitt 1.6 des UC-Templates: Use case conditions 43
Tabelle 17: Abschnitt 1.8 des UC-Templates: General remarks 44
Tabelle 18: Abschnitt 2 des UC-Templates: Diagram of use case 44
Tabelle 19: Abschnitt 3.1 des UC-Templates: Actors 44
Tabelle 20: Erweiterter Abschnitt 3.2 des UC-Templates: Actors 45
Tabelle 21: Abschnitt 4 des UC-Templates: Overview of scenarios 45
Tabelle 22: Abschnitt 4.2 des UC-Templates: Steps - Scenarios 45
Tabelle 23: Abschnitt 5 des UC-Templates: Information exchanged 46
Tabelle 24: Erweiterter Abschnitt 5 des UC-Templates: Information exchanged 47
Tabelle 25: Abschnitt 6 des UC-Templates: Requirements (optional) 47
Tabelle 26: Anpassungen Abschnitt 3.1 – Actors 48

Tabelle 27: Anpassungen Abschnitt 5 – Information Exchanged 48
Tabelle 28: Auswirkungen der Empfehlungen auf Abschnitte des Use Case-Templates 50

Ergebnisdokument AS 12.2.17

„Schulung und Sensibilisierung“

Autoren:

Dennis Beer (AS-Verantwortlicher, EWE Netz), Konrad Rosmus (IABG),
Ulrike Henschel (IABG), Marie Clausen (OFFIS), Christine Rosinger (OFFIS)

10.12.2020

SINTEG
SCHAUFENSTER INTELLIGENTE ENERGIE

Gefördert durch:

Bundesministeri
für Wirtschaft
und Energie

aufgrund eines Beschlu
des Deutschen Bundest

Historie des Dokuments:

Version	Datum	Name	Änderungen	Dateiname
0.01	20.03.2020	Henschel	Erstfassung	20200320_AS12.2.17_Schulung und Sensibilisierung_V0.01.docx
0.02	25.03.2020	Henschel	Anpassungen nach AP12-Treffen (virtuell)	20200325_AS12.2.17_Schulung und Sensibilisierung_V0.02.docx
0.02	10.08.2020	Clausen	Ergänzung: Beispiel Point-and-Click-Adventure	20200325_AS12.2.17_Schulung und Sensibilisierung_V0.02_MCl.docx
0.03	18.09.2020	Henschel	Umsetzung von Anmerkungen OFFIS, Ergänzungen und neue Kapitel zu div. Themen und Beispielen	20200918_AS12.2.17_Schulung und Sensibilisierung_V0.03.docx
0.04	02.10.2020	Henschel	Umsetzung von QS-Anmerkungen und Input (IABG, OFFIS); Kapitel zum e-Training SiLKe ergänzt.	20201002_AS12.2.17_Schulung und Sensibilisierung_V0.04.docx
0.05	08.10.2020	Henschel	Ergänzung zum Thema Pseudo-Vorfall	20201008_AS12.2.17_Schulung und Sensibilisierung_V0.05.docx
1.0	10.12.2020	Henschel, IABG	Finalisierung zur Freigabe als Version 1.0	20201210_AS12.2.17_Schulung und Sensibilisierung_V1.0.docx

Inhalt

Abkürzungsverzeichnis 4
1 Einordnung und Ziele 7
2 Zusammenfassung und Gliederung 8
3 Aufgabenstellung und Vorgehensweise 10
3.1 Vorgehensweise und Ziele im AS 12.2.17 10
3.2 Ziele und Anforderungen im IT-Grundschutz zu „Sensibilisierung und Schulung“ 10
4 Sensibilisierung des Managements für Aspekte der Informationssicherheit 14
4.1 Zielgruppenanalyse (Management) 15
4.1.1 Voraussetzungen und Annahmen 15
4.1.2 Anforderungen hinsichtlich der Trainingsformate 16

4.2 Zu vermittelnde Inhalte (Management) 17
4.2.1 Aufteilung in thematische Einheiten 19
4.2.2 Vertiefung von Inhalten mit Unternehmensbezug 19
4.2.3 Wichtige Inhalte mit Bezug zum persönlichen Verhalten 20
4.3 Zielgruppengerechte Vermittlung der Inhalte (Management) 20
4.4 Sicherheitskultur im Unternehmen 21
5 Methoden und Techniken im Überblick 22
5.1.1 Unterschiedliche Formate und Bezeichnungen 22
5.1.2 Einzelne Aspekte von Schulungsveranstaltungen: Vor- und Nachteile 23
5.1.3 Der besondere Stellenwert der Gamification 29
6 Schulung und Sensibilisierung zur Informationssicherheit: Beispiele 31
6.1 Escape Game / Escape Room 31
6.1.1 Format 31
6.1.2 Beispiel „Escape Room“ (EWE) 31
6.2 Point-and-Click-Adventure 32
6.2.1 Format 32
6.2.2 Beispiel Point-And-Click-Adventure (OFFIS, noch unbenannt) 32
6.3 Game of Threats™ – Cyber Security-Simulation für Manager 33
6.3.1 Format 33
6.3.2 Beispiel Game of Threats auf einer Messe 33
6.4 Cyber Range 35
6.4.1 Format 35
6.4.2 Beispiel „CyberRange-e: Cybersecurity für Stromnetze“ 35
6.5 Rollenspiel (Simulation) 36
6.5.1 Format 36
6.5.2 Themenvorschläge für konkrete Rollenspiele 37
6.5.3 Thema “Social Hacking” als Ausgangspunkt für weitere Rollenspiele 41
6.6 Coaching (on the job) 44
6.7 Enera-Lernplattform 44
6.7.1 Format des Angebotes 44
6.7.2 Beispiel eTraining „Informationssicherheit“ 45
6.7.3 Beispiel eTraining „Informationssicherheit KRITIS“ 45
6.7.4 Beispiel eTraining „Sichere Lieferkette (SiLKe)“ 46

6.8 Weitere Möglichkeiten zur Sensibilisierung und Motivation für Sicherheitsthemen . 46
6.8.1 Vertrauliche Meldewege 47
6.8.2 Newsletter und Events 47
6.8.3 Objekte, Bilder und Symbole 48
6.8.4 Inszenierung von Pseudo-Vorfällen 49
6.8.5 “Lessons Learned” / Debriefing 50
7 Scope-übergreifend relevante Erkenntnisse, Ergebnisse und Festlegungen 51
7.1 Attraktivität von Kursen zur Informationssicherheit 51
7.2 Interesse an Sicherheitsthemen in anderen enera-Arbeitspaketen 51
8 Zusammenfassung und Ausblick 51
9 Anlagen 53
10 Bezugsdokumente 54
11 Abbildungsverzeichnis 57
12 Tabellenverzeichnis 57

Abkürzungsverzeichnis

Abkürzung	Bedeutung
AP	Arbeitspaket
AS	Arbeitsschritt
BDSG	Bundesdatenschutzgesetz
BCM	Business Continuity Management
BMWi	Bundesministerium für Wirtschaft und Energie
BNetzA	Bundesnetzagentur
BSI	Bundesamt für Sicherheit in der Informationstechnik
BYOD	Bring Your Own Device *Bezeichnung für die Integration privater Endgeräte in die Netzwerke von Unternehmen oder anderen Institutionen.*
CLS	Controllable Local System
DoS	Denial of Service
EE	Erneuerbare Energien
EEG	Erneuerbare-Energien-Gesetz
EnWG	Energiewirtschaftsgesetz
EU	Europäische Union

Abkürzung	Bedeutung
EU-DSGV	EU Datenschutzgrundverordnung
GWA	(Smart-Meter-) Gateway-Administrator
GWA-S	(Smart-Meter-) Gateway-Administrationssystem
GWH	(Smart-Meter-) Gateway-Hersteller
ID	Identifikator
ICS	Industrial Control Systems (Automatisierungs-, Prozesssteuerungs- und Prozessleitsysteme)
IEC	International Electrotechnical Commission, deutsch: Internationale Elektrotechnische Kommission
IH	Incident Handling
IKT	Informations- und Kommunikationstechnik
IS	Informationssicherheit
ISMS	Informationssicherheitsmanagementsystem, englisch: Information Security Management System
ISO	International Organization for Standardization, deutsch: Internationale Organisation für Normung
IT	Information Technology (Informationstechnik)
ITGS	IT-Grundschutz
IV	Informationsverbund (*IT-Grundschutz, entspricht „Scope“ in ISO 2700x)*
KRITIS	Kritische Infrastrukturen
MSB	Messstellenbetreiber
NIS	Netz- und Informationssicherheit
NIST	National Institute of Standards and Technology
NISTIR	NIST Internal/Interagency Report
OT	Operative Technologien (Betriebstechnik)
SB	Schutzbedarf
SDSP	Smart Data and Service Platform
SGAM	Smart Grid Architecture Model
SGIS	Smart Grid Information Security
SGO	Smart Grid Operator
SiLKe	Sichere Lieferkette (für SMGW)
SMGW	Smart Meter Gateway
SMGWA	Smart-Meter-Gateway-Administrator
SM-PKI	Smart Metering - Public Key Infrastruktur
TAP	Teilarbeitspaket

Abkürzung	Bedeutung
TR	Technische Richtlinie
UC	Use Case
UCMR	Use Case Management Repository
ÜNB	Übertragungsnetzbetreiber
VK	Virtuelles Kraftwerk
VPP	Virtual Power Plant

Ergebnisdokument AS 12.2.17

„Schulung und Sensibilisierung“

1 Einordnung und Ziele

Enera ist eins der fünf durch das Bundesministeriums für Wirtschaft und Energie (BMWi) geförderten Projekte des Förderprogramms „Schaufenster intelligente Energie – Digitale Agenda für die Energiewende“ (SINTEG)[1]. Im Projekt werden Lösungen zu den drei Themenschwerpunkten Netz, Markt und Daten in der Modellregion im Nordwesten Niedersachsens entwickelt und erprobt. Das **Arbeitspaket (AP) 12** innerhalb dieses Projekts beschäftigt sich mit der informationstechnischen Entwicklung der enera Gesamtarchitektur inklusive eines Informationssicherheitskonzepts.

Das Teilarbeitspaket (TAP) 12.2 befasst sich mit dem Informationssicherheitskonzept.

Der dazugehörige Arbeitsschritt (AS) 12.2.17 „**Schulung und Sensibilisierung**“ setzt sich innerhalb dieses TAPs mit ausgewählten Aspekten einer möglichst effizienten und nachhaltig wirksamen Vermittlung sicherheitsrelevanter Informationen und Verhaltensweisen auseinander, durch die das Informationssicherheitskonzept und das zugehörige Informationsmanagementsystem (ISMS) im Unternehmen und im Arbeitsalltag „verankert“ werden.

Insofern beschäftigt sich der AS 12.2.17 „Schulung und Sensibilisierung“ also mit flankierenden Maßnahmen zu den Arbeitsschritten 12.2.7 bis 12.2.12 (siehe Abbildung 1), die bei der Einführung eines ISMS zunächst im Mittelpunkt stehen.

Abbildung 1 stellt die Abhängigkeiten der einzelnen Arbeitsschritte in TAP 12.2 im Überblick dar.

[1] Siehe auch die Seite des SINTEG-Förderprogramms auf der Homepage des BMWi https://www.bmwi.de/Redaktion/DE/Artikel/Energie/sinteg.html.

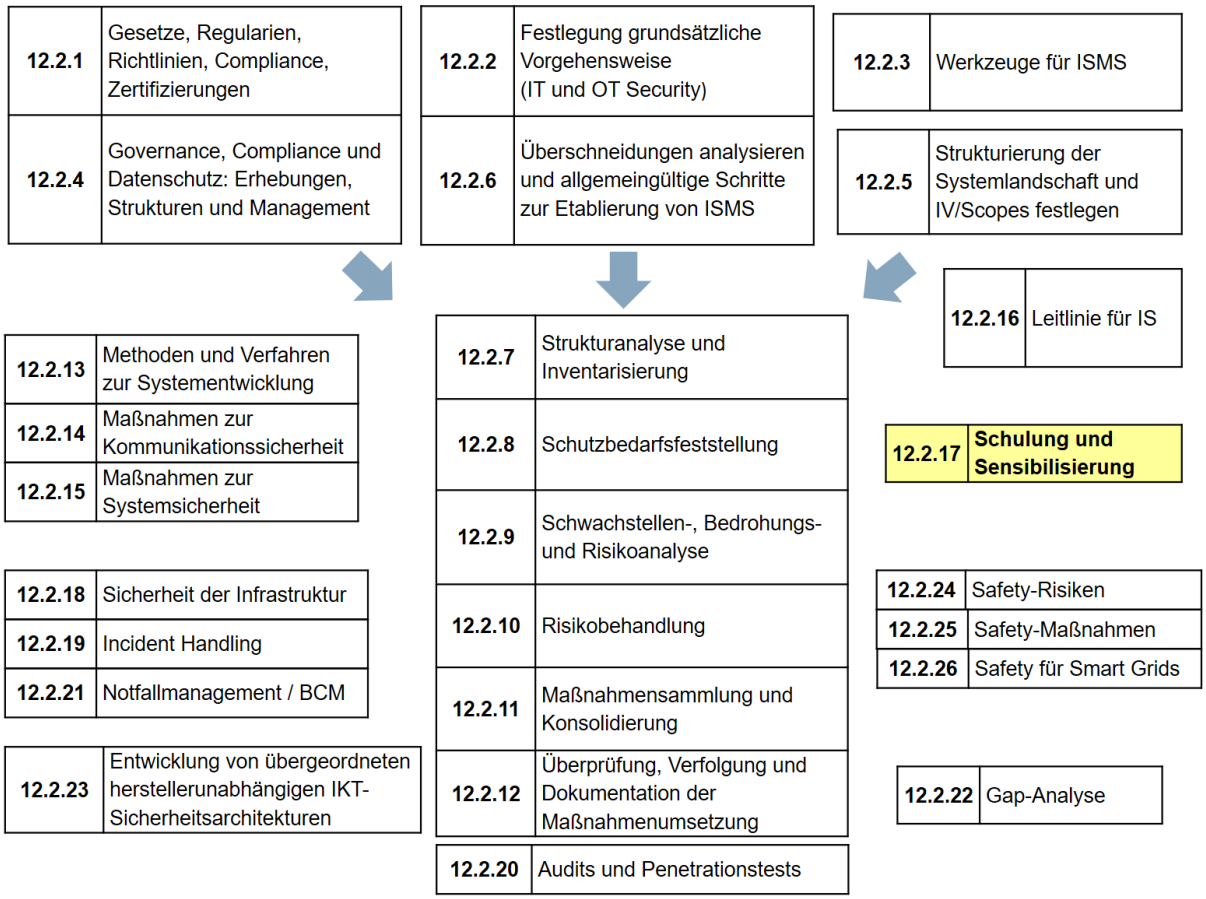


Abbildung 1: Abhängigkeit der Arbeitsschritte in TAP 12.2 zur Einführung des enera-ISMS

Da bei der Durchführung der Arbeitsschritte unterschiedliche Vorgehensweisen möglich sind, wurden sie zum Teil spezifisch für einzelne Informationsverbünde (Scopes) durchgeführt. Eine solche Differenzierung wird im Arbeitsschritt AS 12.2.17 „Schulung und Sensibilisierung“ nicht vorgenommen, da im Schwerpunkt nur übergreifend bzw. querschnittlich relevante Themen, Zielsetzungen und Zielgruppen betrachtet werden.

2 Zusammenfassung und Gliederung

Im AS 12.2.17 geht es um das Thema „Schulung und Sensibilisierung“ zu Sicherheitsthemen. Nur wenn die Gefährdungen und Risiken im Bereich der Informationssicherheit allen Mitarbeitern eines Unternehmens bekannt und bewusst sind, und nur wenn diese mit angemessenen und eingeübten Verhaltensweisen damit umgehen bzw. darauf reagieren können, kann ein angestrebtes Sicherheitsniveau erreicht werden – technische Maßnahmen alleine reichen

hierzu nicht aus[2]. Hieraus ergibt sich der hohe Stellenwert des Themas „Schulung und Sensibilisierung“, und das Erfordernis, dieses möglichst wirksam und effizient umzusetzen. Dazu tragen eine sorgfältige Zielgruppenanalyse, die Auswahl geeigneter Inhalte und der Einsatz passender Methoden und Techniken wesentlich bei.

- In Kapitel 3 werden **Aufgabenstellung und Vorgehensweise** für AS 12.2.17 dargestellt, wobei auch auf einzelne Voraussetzungen im Projekt enera eingegangen wird. Einen Schwerpunkt bilden die Vorgaben im Baustein ORP.3 „Sensibilisierung und Schulung“ im IT-Grundschutz-Kompendium des BSI [10].

- Kapitel 4 befasst sich exemplarisch mit der Sensibilisierung der **Zielgruppe „Management“** für Sicherheitsfragen. Dem Management kommt im Kontext eines unternehmensweiten Informationssicherheitsmanagement eine Schlüsselrolle zu, sowohl als Vorbild als auch bei der Steuerung von Ressourcen. Hierauf wird bei der **Zielgruppenanalyse** und der Auswahl relevanter **Schulungsinhalte** sowie der zielgruppengerechten **Vermittlung** näher eingegangen. Abschließend wird der Stellenwert der **Sicherheitskultur im Unternehmen** thematisiert.

- Kapitel 5 gibt einen Überblick über die verfügbaren **Methoden und Techniken** zur Vermittlung der im vorausgehenden Kapitel angesprochenen Inhalte. Einzelne Aspekte von Schulungsveranstaltungen werden im Hinblick auf ihre Einsatzmöglichkeiten beschrieben und bewertet. Entsprechend ihrem besonderen Stellenwert wird auf die „Gamification“ vertiefend eingegangen.

- In Kapitel 6 wird eine Auswahl von **Beispielen aus dem „Bereich Schulung und Sensibilisierung zur Informationssicherheit**“ vorgestellt. Dabei liegt der Schwerpunkt auf besonderen Schulungsformaten, die die Teilnehmer durch neuartige und unkonventionelle Methoden und Techniken motivieren und ansprechen sollen; Ziel ist es, hierdurch einen möglichst nachhaltigen Sensibilisierungs- und Lerneffekt zu erreichen. Weitere Beispiele stellen Möglichkeiten zur Sensibilisierung und Motivation für sicherheitsgerichtetes Verhalten im Bereich der Unternehmenskultur vor.

- Kapitel 7 enthält zusammenfassend wesentliche **Erkenntnisse, Ergebnisse und Festlegungen** aus dem AS 12.2.17.

- Abschließend enthält Kapitel 8 eine **Bewertung der Vorgehensweisen**, die im AS 12.2.17 eingesetzt wurden, sowie einen **Ausblick** auf benachbarte Arbeitsschritte im Teilarbeitspaket 12.2.

[2] Ein bekanntes Zitat von Bruce Schneier (US-Amerikanischer Sicherheits-Experte) lautet: „Wenn Sie glauben, Technologie könne Ihre Sicherheitsprobleme [alleine] lösen, dann verstehen Sie die Probleme nicht, und die Technologie verstehen Sie [auch] nicht.“ bzw. “If you think technology can solve your security problems, then you don’t understand the problems and you don’t understand the technology.” Bruce Schneier, Vorwort zu “Secrets and Lies” (2000), siehe https://de.wikipedia.org/wiki/Bruce_Schneier.

3 Aufgabenstellung und Vorgehensweise

> *Gedacht heißt nicht immer gesagt,/ gesagt heißt nicht immer richtig gehört,/ gehört heißt nicht immer richtig verstanden,/ verstanden heißt nicht immer einverstanden,/ einverstanden heißt nicht immer angewendet,/ angewendet heißt noch lange nicht beibehalten.* (Konrad Lorenz)

In den Arbeitsschritten 12.2.7 bis 12.2.12 wurde bezogen auf ausgewählte Bereiche bzw. „Scopes“ des Informationsverbundes enera ein exemplarisches Informationssicherheitsmanagementsystem (ISMS) entworfen. Um ein solches ISMS mit „Leben“ zu erfüllen, ist es erforderlich, alle Mitarbeiter in die Lage zu versetzen, die bestehenden Sicherheitsanforderungen umzusetzen bzw. die resultierenden Regeln zu beachten und zu befolgen. Anforderungen und Regeln können in Schulungen, Trainings, Einweisungen usw. vermittelt werden, sie reichen alleine jedoch nicht aus, da nicht alle Gefährdungen und Risiken immer vollständig vorhersehbar sind. Deshalb ist ergänzend auch eine Sensibilisierung der Mitarbeiter wichtig, bei der ihr Bewusstsein für bzw. ihre Wahrnehmung von Gefährdungen und Risiken erhöht wird, so dass sie ggf. eigenständig eine angemessene Verhaltensweise wählen können.

3.1 Vorgehensweise und Ziele im AS 12.2.17

Im Arbeitsschritt 12.2.17 „Schulung und Sensibilisierung“ wird hierzu genauer untersucht, welche Schulungs- und Sensibilisierungsbedarfe grundsätzlich bestehen bzw. vordringlich zu erfüllen sind. Eine solche Analyse beginnt mit der Identifikation der Zielgruppe und deren besonderen Voraussetzungen und Bedarfe. Auf dieser Basis erfolgt die Identifikation und Zusammenstellung der spezifischen zu vermittelnden Inhalte. Die Auswahl dazu passender geeigneter Vermittlungs-Methoden und -techniken erfolgt im Zusammenhang mit einer Bewertung der verfügbaren bzw. gängigen Lehr- und Trainings-Methoden und -techniken. Da sich diese i. d. R. nicht immer als ausreichend erweisen, sollen einzelne besondere Lehr- und Trainingsformen intensiver betrachtet und durch Beispiele vorgestellt werden.

Im folgenden Unterkapitel werden ergänzend die Zielsetzungen und Anforderungen im Bereich „Schulung und Sensibilisierung“ dargestellt, die aus Sicht des IT-Grundschutz [10] – einer wesentlichen Grundlage für ein ISMS – hierzu bestehen.

3.2 Ziele und Anforderungen im IT-Grundschutz zu „Sensibilisierung und Schulung“

Im IT-Grundschutz-Kompendium des BSI [10] behandelt der Baustein **ORP.3** das Thema **„Sensibilisierung und Schulung“**. Die Mitarbeiter eines Unternehmens werden als wesentlicher Erfolgsfaktor für die effiziente und erfolgreiche Umsetzung von Informationssicherheit angesehen. Erforderlich hierzu sind Aufbau und Gestaltung einer Sicherheitskultur im Unternehmen, die bei den Mitarbeitern zu Sicherheitsbewusstsein (Awareness) führt. Insbesondere muss jeder Mitarbeiter

- für relevante Gefährdungen sensibilisiert sein und wissen, wie sich diese auf das Unternehmen auswirken können,
- die eigene Rolle im Informationssicherheitsmanagement des Unternehmens kennen und wissen, was im Hinblick auf Informationssicherheit von den Mitarbeitern erwartet wird,
- die vorgegebenen Sicherheitsmaßnahmen kennen und wissen und wie diese anzuwenden sind,
- wissen, welche besonderen Reaktionen in sicherheitskritischen Situationen erforderlich sind,
- insgesamt bereit sein, die Sicherheitsmaßnahmen wirkungsvoll zu unterstützen.

Neben der **Vermittlung von Informationen** wird hier also auch der **Motivation** ein hoher Stellenwert beigemessen.

Die prozessualen, technischen, methodischen und organisatorischen Anforderungen an die Sensibilisierung und Schulung zur Informationssicherheit, die im ITGS-Baustein ORP.3 beschrieben werden, beziehen sich mit Schwerpunkt darauf, wie ein planvolles, zyklisches und organisatorisches Vorgehen hierzu effizient gestaltet werden kann. **Konkrete Schulungsinhalte** können aus anderen, jeweils themenspezifischen IT-Grundschutz-Bausteinen entnommen werden. Als elementare Gefährdungen, vor denen Schulung und Sensibilisierung letztlich schützen sollen, werden im ITGS-Baustein ORP.3 die folgenden besonders hervorgehoben:

- G 0.14 Ausspähen von Informationen (Spionage)
- G 0.15 Abhören
- G 0.19 Offenlegung schützenswerter Informationen
- G 0.24 Zerstörung von Geräten oder Datenträgern
- G 0.29 Verstöße gegen Gesetze und Regelungen
- G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen
- G 0.32 Missbrauch von Berechtigungen
- G 0.36 Identitätsdiebstahl
- G 0.37 Abstreiten von Handlungen
- G 0.38 Missbrauch personenbezogener Daten
- G 0.42 Social Engineering
- G 0.45 Datenverlust
- G 0.46 Integritätsverlust schützenswerter Informationen

Neben den bereits genannten Aspekten wird im Baustein ORP.3 deutlich herausgearbeitet, welche Ursachen den Erfolg gezielter Aktivitäten zur Schulung und Sensibilisierung behindern können, bzw. dass die folgenden **Erfolgsfaktoren** wesentlich sind:

- Ausreichende Management-Unterstützung,
- Klare Ziele,
- Gute Planung,
- Erfolgskontrolle,
- Kontinuität,

- Ausreichende finanzielle und personelle Ressourcen.

Bei der **Analyse der Gefährdungslage** im Hinblick auf ein erfolgreiches Informationssicherheitsmanagement insgesamt werden im Baustein ORP.3 entsprechend dem oben Gesagten die folgenden spezifischen Gefährdungen besonders hervorgehoben und erläutert:

1. Unzureichende Kenntnis über Regelungen: Insbesondere den Funktionsträgern müssen die geltenden Regelungen bekannt sein.
2. Unzureichende Sensibilisierung für Informationssicherheit: Es reicht nicht, Sicherheitsmaßnahmen nur anzuordnen, sondern deren Bedeutung und Zweck sollten den Mitarbeitern bekannt sein.
3. Unwirksame Aktivitäten zur Sensibilisierung und Schulung: Diese Gefahr besteht, falls die o. g. Erfolgsfaktoren nicht oder nicht ausreichend gegeben sind.
4. Unzureichende Schulung der Mitarbeiter zu Sicherheitsfunktionen: z. B. bei neu eingeführter Software.
5. Nicht erkannte Sicherheitsvorfälle: Wenn Mitarbeiter und Administratoren nicht ausreichend geschult und sensibilisiert sind, werden Sicherheitsvorfälle evtl. erst verspätet oder gar nicht erkannt.
6. Nichtbeachtung von Sicherheitsmaßnahmen: Durch Unachtsamkeit und Hektik werden Sicherheitsmaßnahmen umso weniger beachtet, je weniger sie durch gute Schulung und Sensibilisierung verankert sind.
7. Sorglosigkeit im Umgang mit Informationen: Hier reichen technische Sicherheitsmaßnahmen nicht aus, sondern es kommt auf das Sicherheitsbewusstsein der Mitarbeiter an.
8. Fehlende Akzeptanz von Informationssicherheitsvorgaben: Gründe können in einer fehlenden Sicherheitskultur und einer fehlenden Vorbildfunktion durch die Institutionsleitung, aber auch in übertriebenen – oder als solchen angesehenen – Sicherheitsanforderungen.
9. Social Engineering: Nur durch ausreichende Sensibilisierung können Mitarbeiter und somit die Institution in dieser Hinsicht geschützt werden.

Die erste Anforderung ORP.3.A.1 im Baustein ORP.3 trägt die Überschrift: „Sensibilisierung der Institutionsleitung für Informationssicherheit“, und sie richtet sich an alle Vorgesetzten bzw. das gesamte Management einer Institution (im IT-Grundschutz wird das Management als „Institutionsleitung“ bezeichnet). Es handelt sich um eine sog. Basis-Anforderung, das heißt, sie muss in jedem ISMS unabhängig von dessen Umfang oder Ausbaustufe und unabhängig von der Höhe des Schutzbedarfes auf jeden Fall erfüllt werden:

ORP.3.A1 Sensibilisierung der Institutionsleitung für Informationssicherheit [Vorgesetzte, Institutionsleitung]

Die Institutionsleitung MUSS die Sicherheitskampagnen und Schulungsmaßnahmen für die Mitarbeiter unterstützen. Daher MUSS vor dem Beginn eines Sensibilisierungs-

> und Schulungsprogramms zur Informationssicherheit die Unterstützung der Institutionsleitung eingeholt werden. Die Institutionsleitung MUSS ausreichend für Sicherheitsfragen sensibilisiert werden.
>
> Alle Vorgesetzten MÜSSEN die Informationssicherheit unterstützen, indem sie mit gutem Beispiel vorangehen. Führungskräfte MÜSSEN die Sicherheitsvorgaben umsetzen. Hierüber hinaus MÜSSEN sie ihre Mitarbeiter auf deren Einhaltung hinweisen.
>
> Quelle: ITGS-Kompendium [10]

Die Umsetzung dieser Anforderung, insbesondere der Anteil „Sensibilisierung", wird im Arbeitsschritt AS 12.2.17 ausführlich thematisiert, siehe Kapitel 4 in diesem Dokument.

Die weiteren Anforderungen im Überblick:

- ORP.3.A2 Ansprechpartner zu Sicherheitsfragen
- ORP.3.A3 Einweisung des Personals in den sicheren Umgang mit IT
- ORP.3.A4 Konzeption eines Sensibilisierungs- und Schulungsprogramms zur Informationssicherheit
- ORP.3.A5 Analyse der Zielgruppen für Sensibilisierungs- und Schulungsprogramme
- ORP.3.A6 Planung und Durchführung von Sensibilisierungen und Schulungen zur Informationssicherheit
- ORP.3.A7 Schulung zur Vorgehensweise nach IT-Grundschutz
- ORP.3.A8 Messung und Auswertung des Lernerfolgs
- Bei erhöhtem Schutzbedarf:
  ORP.3.A9 Spezielle Schulung von exponierten Personen und Institutionen

Erläuterungen zu diesen Anforderungen finden sich im ITGS-Kompendium [10] selbst, und es gibt zu den Anforderungen auch bereits auf das ITGS-Kompendium abgestimmte Umsetzungshinweise [10] des BSI. Die ersten der bei den Umsetzungshinweisen beschriebenen Maßnahmen beziehen sich auf die oben vorgestellte Anforderung ORP.3.A1 „Sensibilisierung der Institutionsleitung[3] für Informationssicherheit"; mehr hierzu siehe das folgende Kapitel 4, in dem es um die Sensibilisierung des Managements[3] für die wesentlichen Aspekte der Informationssicherheit geht.

[3] Die Begriffe „Institutionsleitung" und „Management" werden im vorliegenden Ergebnisbericht als gleichbedeutend verstanden. Die ITGS-Anforderung wurde in der aktuellen Edition 2020 des ITGS-Kompendium [10] umbenannt von „Sensibilisierung des Managements für Informationssicherheit" zu „Sensibilisierung der Institutsleitung für Informationssicherheit". Da die aktuellsten Umsetzungshinweise noch aus der Edition 2019 des ITGS-Kompendiums stammen, wird dort der Begriff „Management" verwendet.

4 Sensibilisierung des Managements für Aspekte der Informationssicherheit

Es ist nur dann möglich, Informationssicherheit innerhalb einer Institution erfolgreich und effizient zu verwirklichen, wenn alle Mitarbeiter erkennen und akzeptieren, dass sie ein bedeutender und notwendiger Faktor für den Erfolg der Institution sind und wenn sie bereit sind, Sicherheitsmaßnahmen wirkungsvoll zu unterstützen. Hierfür müssen eine Sicherheitskultur und ein Sicherheitsbewusstsein (Awareness) aufgebaut und gepflegt werden. Mitarbeiter müssen für relevante Gefährdungen sensibilisiert werden und wissen, wie sich diese auf ihre Institution auswirken können, denn je mehr ihnen Risiken bekannt sind, desto eher akzeptieren sie entsprechende Sicherheitsmaßnahmen. Sie müssen auch über die erforderlichen Kenntnisse verfügen, um Maßnahmen richtig verstehen und anwenden zu können. Insbesondere muss ihnen bekannt sein, was von ihnen im Hinblick auf Informationssicherheit erwartet wird und wie sie in sicherheitskritischen Situationen reagieren sollten.

Um den Mitarbeitern das nötige Wissen zu vermitteln, sind gleichermaßen Sensibilisierungs- und Schulungsmaßnahmen erforderlich. Ziel der Sensibilisierung für Informationssicherheit ist es, die Wahrnehmung der Mitarbeiter für sicherheitskritische Situationen und ihre Auswirkungen zu schärfen. Durch Schulungen zur Informationssicherheit sollen die Mitarbeiter die notwendigen Kenntnisse und Kompetenzen für sicherheitsbewusstes Verhalten im beruflichen und privaten Umfeld erwerben.

Eine angemessene Informationssicherheit sollte von allen Mitarbeitern als selbstverständlicher Teil ihrer Arbeitsumgebung verinnerlicht werden. Dies setzt in vielen Bereichen eine langfristige Verhaltensänderung voraus, besonders wenn Informationssicherheit mit Komfort- oder Funktionseinbußen verbunden ist. Um hier nachhaltige Ergebnisse zu erzielen, ist ein kontinuierlicher Prozess erforderlich. Daher muss die Institution ein durchgängiges Sensibilisierungs- und Schulungsprogramm zur Informationssicherheit erarbeiten und etablieren. Es sollte bereits bei der Einstellung von Mitarbeitern beginnen, unterschiedliche Zielgruppen mit deren Fähigkeiten, Arbeitsabläufen und benötigten Ressourcen berücksichtigen und die Mitarbeiter auch begleiten, wenn sich ihre Aufgaben oder Positionen verändern.[4]

Bereits im Vorfeld des Arbeitsschrittes 12.2.17 wurde die Zielgruppe „Management“ als von besonderem Interesse für diesen Arbeitsschritt identifiziert, da deren Angehörige – z. B. als Informationsträger oder auf Dienstreisen – überdurchschnittlichen Risiken ausgesetzt sein können. Außerdem sollen sie Vorbild-Funktionen im Unternehmen ausüben und auch über Ressourcen und Budgets entscheiden, die direkte Auswirkungen auf die Informationssicherheit haben können. Andererseits können sie i. d. R. nur wenig Zeit für Schulungen und Trainings erübrigen. Diese sollten daher entsprechend motivierend und wirksam sein.

[4] Diese Ausführungen entsprechen (etwas umformuliert) den Umsetzungshinweisen zum Baustein „ORP.3 Sensibilisierung und Schulung“ im ITGS-Kompendium 2. Edition 2019 [10].

Die Sensibilisierung des Managements für Sicherheitsfragen ist auch eine wesentliche Anforderung im IT-Grundschutz des BSI [10], im Hinblick auf Sensibilisierung und Schulung aller Mitarbeiter eines Unternehmens (siehe Kapitel 3.2).

Das Thema „Sicherheit“ bzw. einzelne Sicherheitsthemen dürfen dabei nicht nur initial, einmalig und ausschnittsweise vermittelt werden, sondern für eine erfolgreiche und dauerhafte Sensibilisierung und Schulung müssen die Themen bei allen Verantwortlichen immer wieder möglichst aktuell und präsent gehalten werden, wobei Interesse und Motivation als entscheidende Erfolgsfaktoren die Wahl der Methoden bestimmen.

In den folgenden Unterkapiteln folgt nach einer Zielgruppenanalyse des Managements in Abschnitt 4.1 zunächst ein Überblick über die wesentlichen Schulungs- und Sensibilisierungsinhalte für diese Zielgruppe in Abschnitt 4.2. Daran schließen Empfehlungen zur zielgruppengerechter Vermittlung dieser Inhalte in Abschnitt 4.3 an. Abschnitt 4.4 befasst sich abschließend mit der Sicherheitskultur als unternehmensweiter Aufgabe für das Management und dem entsprechenden Sensibilisierungsbedarf.

4.1 Zielgruppenanalyse (Management)

In einem Schulungs- und Sensibilisierungskonzept bildet die Zielgruppenanalyse die Grundlage dafür, dass ggf. auf besondere Voraussetzungen eingegangen werden kann und die relevanten Inhalte ausgewählt und in geeigneter Form vermittelt werden. Bei den Zielgruppen werden häufig die folgenden unterschieden:

- Management- / Institutsleitungs-Ebene,
- Mitarbeiter (allgemein),
- Administratoren,
- Personalabteilung, ggf. weitere besondere Abteilungen wie z. B. eine Pressestelle,
- Externe Projektmitarbeiter,
- Neueinstellungen.

Bei dieser Aufteilung ist zu beachten, dass sie nicht disjunkt zu verstehen ist – ein einzelner Mitarbeiter gehört also i. d. R. zu mehreren Zielgruppen. Während die Zielgruppen „Administratoren“, „Personalabteilung“ usw. gewöhnlich durch Maßnahmen berücksichtigt werden, die diejenigen für die Zielgruppe „Mitarbeiter“ ergänzen, wird die Zielgruppe „Management“ häufig als eigenständige betrachtet. Sie hat zwar in Bezug auf zu vermittelnde Inhalte vieles mit der Zielgruppe „Mitarbeiter“ gemeinsam, aufgrund besonders gearteter zeitlicher und organisatorischer Voraussetzungen ist jedoch bei der Vermittlung der Inhalte ein spezifisches Vorgehen erforderlich.

Ein Beispiel für eine detaillierte Zielgruppenanalyse findet sich in Anlage 2 zu diesem Dokument.

4.1.1 Voraussetzungen und Annahmen

Für die Zielgruppe „Management“ gelten die folgenden Voraussetzungen bzw. es werden die folgenden Annahmen getroffen:

Aufgaben mit Sicherheitsbezug:

- Budgetverantwortung für Sicherheitsthemen,
- Vorbildfunktion für Mitarbeiter,
- Sicherheitsbewusstes Verhalten wie sonstige Büro-Mitarbeiter und IT-Nutzer.

Teilnahme an Maßnahmen zu Schulung und Awareness:

- Verfügbare Zeit ist gering,
- IT-bezogene Vorbildung ist evtl. nur gering bzw. kann nicht vorausgesetzt werden,
- Vertrautheit mit IT-Sicherheitsthemen ist evtl. nur gering bzw. kann nicht vorausgesetzt werden.

Gefährdung / Betroffenheit:

Gefährdung **als Rollenträger im Unternehmen**: hoch

- im Besitz von vertraulichen Informationen,
- als Person potenzielles Ziel von Erpressung, Entführung.

Gefährdung **auf Reisen**: hoch

- häufige Reisen,
- im Besitz sensibler Informationen,
- in potenziell unsicherer Umgebung.

Betroffenheit **als Büromitarbeiter bzw. IT-Nutzer**

- evtl. Unkenntnis bzw. unrealistische Einschätzung von Risiken,
- evtl. fehlende Bereitschaft zur Beachtung subjektiv irrelevanter Vorgaben,
- evtl. fehlende Routine bei der IT-Nutzung.

4.1.2 Anforderungen hinsichtlich der Trainingsformate

Zeitliche Anforderungen

Für die Zielgruppe „Management“ sind kurze, in sich abgeschlossene Einheiten von nicht mehr als 30 bis 40 Minuten empfehlenswert, die ohne allzu große zeitliche „Opfer“ in die relativ eng getakteten Terminpläne von Managern aufgenommen werden können. Als positive Auswirkungen ergeben sich:

- Höhere Bereitschaft bzw. geringere zeitliche „Hemmschwelle“ zur Teilnahme,
- Vermeidung von Aufmerksamtkeitsdefiziten und Demotivation,
- Kürzere Veranstaltungen können häufiger stattfinden und so das Ziel einer kontinuierlichen Awareness fördern sowie thematisch immer auf aktuellem Stand sein.

Allgemeine Anforderungen zu Inhalt und Durchführung

Grundsätzlich sollen Schulungen, Trainings und sonstige Maßnahmen zur Sensibilisierung von Rollenträgern aus dem Management die gleichen inhaltlichen Anforderungen erfüllen, die aus Sicht aller Teilnehmer zu stellen sind:

- Erkennbare Relevanz für die eigene Person, Rolle und Tätigkeit.
- Gute Organisation, Vorbereitung, Qualität der Inhalte und Medien (optisch, technisch usw.).
- Praxisbezogene Beispiele, durch die sich die Teilnehmer „abgeholt" fühlen, und keine abstrakten „Belehrungen" oder „Fachchinesisch". Falls passend, sollten konkrete – und möglichst sofort umsetzbare – praktische Hinweise für den Arbeitsalltag gegeben werden.
- Bilder und Objekte sorgen für mehr Anschaulichkeit als reiner Text, eigenes Handeln erzeugt mehr „Erleben" als rein passives Teilnehmen.
- Beispiele aus der eigenen Arbeitswelt bzw. aus vergleichbaren Unternehmen mit vergleichbaren Aufgaben und Gefährdungen wirken authentischer und ermöglichen Identifikation.
- Vermittlung der Themen mit einer Beispiel-Auswahl und in einer Weise, die einerseits einen möglichst intensiven emotionalen Bezug ermöglicht (Identifikation, Engagement) ohne jedoch andererseits zu ängstigen oder sonstige (auch unbewusste) Abwehr zu erzeugen.
- Erfolgserlebnisse motivieren – entsprechende Aufgaben stellen, wie z. B. Quizfragen.
- Möglichkeit zu Teilnehmer-Fragen und -Rückmeldungen geben, sowohl während einer Veranstaltung in der Runde der Teilnehmer als auch im Anschluss geschützt, ggf. anonym. Feedback aufnehmen, auswerten, ggf. durch weitere Nachfragen ergänzen.

4.2 Zu vermittelnde Inhalte (Management)

Schulung und Sensibilisierung müssen alle relevanten Themen mit Sicherheitsbezug im Unternehmen aufgreifen. Diese Themen ergeben sich u. a. aus der Sicherheitsleitlinie, aus den Anforderungen des ISMS, des Risikomanagements, des Incident Handling (IH) und des Notfallmanagements bzw. Business Continuity Managements (BCM).

Entsprechend der „alltäglichen" Relevanz sollten u. a. die folgenden Themen nicht nur für die Zielgruppe „Management" in Schulungen zur Informationssicherheit angesprochen werden:

- Passwort-Regeln (Auswahl, Umgang mit),
- Schutz von Dokumenten vor Einsicht (Herumliegen lassen, Drucker usw.),

- Zugang zu Rechnern (Sperren bei Abwesenheit, An- und Abmelden),
- Social Engineering,
- Umgang mit unbekannten USB-Sticks (auch „herumliegend“ usw.),
- Gewährung von Zutritt und Zugang („Sicherheit vor Höflichkeit“),
- Datenträger-Entsorgung (sensible Daten),
- Verlust von Geräten und Dokumenten,
- Kommunizieren von Sicherheitsvorfällen (Vorgehen, Haftung),
- Gefahren durch Innentäter,
- Urlaubsvertretung,
- Mobile Geräte,
- Viren-Vorsorge,
- Virus-Befall des eigenen Gerätes erkennen und reagieren,
- Nur dienstliche Nutzung der Unternehmens-IT,
- Datensicherung,
- Datenschutz,
- Mobiles Arbeiten,
- BYOD,
- Nutzung Sozialer Netzwerke,
- Cloud Computing,
- Nutzen von und Sicherheitsgewinn durch standardisierte IT (Verzicht auf Ausnahmen, auch beim Management).

Darüber hinaus muss die Zielgruppe „Management“ zu den folgenden Themenbereichen informiert und sensibilisiert werden:

- **Bestehende Sicherheitsrisiken und deren mögliche Auswirkungen**
  Thematisiert werden sollte u. a.:
  - Bestehende Gefährdungen entsprechend aktueller Risikoanalyse,
  - Potenzielle finanzielle und sonstige Auswirkungen – im Energiebereich besonders auch für die Versorgungssicherheit,
  - Konkrete Beispiele von Sicherheitsvorfällen (eigene oder vergleichbare Institution, evtl. aus der eigenen Historie).

- **Auswirkungen von Sicherheitsvorfällen auf kritische Geschäftsprozesse**
  Die möglichen Auswirkungen sollten möglichst konkret und anschaulich dargestellt werden, ohne Detailkenntnisse vorauszusetzen.

- **Gesetzliche Sicherheitsanforderungen**
  In diesem Zusammenhang sollten Themen der Gewährleistung und Haftung mit möglichst konkreten Beispielen vermittelt werden.

- **Informationsmanagementsystem (ISMS), Zertifizierungen**
  Hierzu können auch Aspekte der Vertrauensbildung und evtl. Wettbewerbsvorteile herangezogen werden.

4.2.1 Aufteilung in thematische Einheiten

Die Schulungsinhalte für das Management sollten, wie bei der Zielgruppenanalyse bereits begründet (siehe Kapitel 4.1), in überschaubaren, in sich abgeschlossenen Einheiten von ca. 30 bis 40 Minuten Dauer vermittelt werden. Das jeweilige Schulungsziel einer solchen Einheit sollte klar formuliert und vermittelt werden, ggf. mit Verweis auf thematisch benachbarte vorausgehende oder noch bevorstehende Einheiten.

Eine Einheit kann z. B. eines – ggf. auch zwei – der folgenden allgemeinen Themen in den Mittelpunkt stellen und hierzu informieren, sensibilisieren und die erforderlichen Maßnahmen und Verhaltensweisen vermitteln:

- Wer sind potenzielle Angreifer (Außen-, Innentäter)?
- Was will ein potenzieller Angreifer erreichen (Schaden, Erpressung, …)?
- Wie schützen wir / schütze ich Kundendaten bzw. welche Gefahren drohen für diese?
- Wie schützen wir die Versorgungssicherheit bzw. inwiefern sind wir angreifbar?
- Welche Gefährdungen bestehen im Büroalltag (E-Mail, Social Engineering)?
- Was kann auf einer Dienstreise unter Sicherheitsaspekten alles passieren?
- Wozu braucht man ein ISMS und wie sieht ein gutes ISMS aus?
- Wozu dienen Incident Handling und BCM bzw. Notfallmanagement?
  Hier evtl. auch Zusammenhänge mit GRC thematisieren.
- Schadsoftwarebefall verhindern / erkennen / reagieren.

Die Auflistung hat keinen Anspruch auf Vollständigkeit; zu weiteren Themen siehe auch die folgenden Abschnitte.

4.2.2 Vertiefung von Inhalten mit Unternehmensbezug

Für die Zielgruppe „Management“ sollten die Themen unter solchen Aspekten differenzierter aufbereitet und stärker vertieft werden, die für sie als Rollenträger im Unternehmen besonders relevant sind bzw. für die sie eine besondere Verantwortung tragen. Solche Aspekte können bezogen auf allgemeine Themen z. B. sein:

- Was kann schlimmstenfalls passieren?
- Welche Maßnahmen sind erforderlich?
- Was ist organisatorisch zu regeln?
- Welchen Aufwand erzeugt das?
- Welche Ressourcen sind hierzu erforderlich (finanziell, personell)?

Hilfreich zur Veranschaulichung können hier realitätsnahe Szenarios sein, um eine Bedrohungslage zu verdeutlichen (z. B. Bedrohung durch Innentäter).

Der Stellenwert eines guten ISMS / BCM könnte mit Beispielen belegt werden, auch hinsichtlich der erforderlichen Aufwände, z. B. durch Vergleiche:

- Durchschnittliches Budget für Sicherheitsmaßnahmen bei vergleichbaren Unternehmen, oder z. B. bei Banken.

4.2.3 Wichtige Inhalte mit Bezug zum persönlichen Verhalten

Insbesondere auch wegen der Vorbildfunktion, die Manager im Unternehmen ausüben, haben Sicherheits-Themen mit Bezug zum persönlichen Verhalten einen hohen Stellenwert. Sie sollten mit der gebotenen Eindringlichkeit und Sensibilität vermittelt werden. Hier geht es z. B. um die folgenden Aspekte:

- So wenig persönliche Daten wie möglich öffentlich machen (Social Media usw.), da diese einen Angriff erleichtern können.

- Vermeiden unsicherer Netzwerke und Arbeitsumgebungen,
  Risiken von mobilen Geräten, öffentlichen Netzwerken, öffentlichen Computern (Hotel Lobby), Stellenwert der Verschlüsselung von Information

- Vorgehensweisen, wie tatsächliche Angriffe / Angriffsversuche gemeldet werden können, auf eine Art die kein Unbehagen erzeugt.

- Betonung des hohen Stellenwertes von beispielhaftem / vorbildlichen Verhalten, u.a.:
  - Keine negativen Bemerkungen über Sicherheitsleitlinien!
  - Niemals einen Mitarbeiter nach Login / Passwort o. ä. fragen!

4.3 Zielgruppengerechte Vermittlung der Inhalte (Management)

Besonders wichtig bei der Schulung und Sensibilisierung der Zielgruppe „Management“ ist der Erlebens- und Verhaltensaspekt. So sollten hoch interaktive Formate eingesetzt werden, die möglichst individuell auf die Teilnehmer abgestimmt sind. Die Teilnehmerzahl sollte entsprechend gering gehalten werden: Empfohlen wird auf Management-Ebene eine Gruppengröße von mindestens drei[5] und maximal sechs bis sieben Teilnehmern. Die Inhalte sollten möglichst dem direkten beruflichen Umfeld entnommen sein, um Erlebnis- und Identifikationsaspekte zu stärken. Entsprechend sollte im Idealfall auch der Trainer diesem Umfeld entstammen bzw. über eine intime Innensicht des Unternehmens verfügen, um Themen passend identifizieren und aufbereiten zu können.

[5] Bei weniger als 3 Teilnehmern wäre eher der Begriff „Coaching“ anwendbar.

Ferner ist es wichtig, innerhalb der Maßnahmen zu Schulung und Sensibilisierung zu Sicherheitsthemen auch die Möglichkeit zur Reflektion zu geben. Je nach Inhalt tritt eine der drei folgenden Perspektiven stärker hervor, es sollte jedoch keine ganz ausgelassen werden.

- „Mensch“: Psychologie, Soziales, Empathie.
- „Organisation“: Organisation, Prozesse, Regelungen usw.
- „Technik“: Alle Themen aus den Bereichen Technologie und Technik.

Nach der Durchführung einer Schulung oder eines Trainings ist eine weitere Begleitung der Teilnehmer zweckmäßig, im Idealfall durch einen Trainer, der auch im Arbeitsalltag „mitschwimmt“. Solche individuellen Coachings könnten in kleinen Einheiten zu 15 bis 30 Minuten erfolgen. Dabei kann u. a. geklärt werden, ob alles verstanden wurde, ob sich Fragen ergeben, ob weitere Schritte nötig sind. Es kann aber auch die inhaltliche Umsetzung des Gelernten unterstützt werden.

Der Zeithorizont ist dabei unterschiedlich anzusetzen: Für die dauerhafte Vermittlung von Wissen können einige Tage bis Wochen veranschlagt werden, Änderungen bei Verhalten und Einstellungen benötigen hingegen mehrere Wochen oder Monate.

4.4 Sicherheitskultur im Unternehmen

Unter sozialpsychologischen Gesichtspunkten muss das individuelle Verhalten immer im Kontext des gesamten Systems betrachtet werden. Entsprechend sind Aufbau und Pflege einer wirksamen Sicherheitskultur eine unternehmensweite Aufgabe für das Management. Auch zum Bewusstsein darüber – neben individuellen Verhaltensweisen und wirtschaftlichen Risiken – sollte die Sensibilisierung dieser Zielgruppe beitragen.

Notwendige Voraussetzungen für eine erfolgreiche Sicherheitskultur sind die folgenden[6]:

- **Wissen**
  Die Methoden und die Gründe möglicher Gefährdungen (z. B. durch Phishing, Social Hacking, usw.) müssen „erlebbar“ bekannt sein.
- **Emotionen**
  Sicherheitsgerichtetes Verhalten muss sich für jeden Mitarbeiter und jede Mitarbeiterin gut und richtig anfühlen.
- **Motivationen**
  Sicherheitsgerichtetes Verhalten müssen alle wollen, und es sollte Spaß machen.
- **Kognitionen**
  Die Sinnhaftigkeit von Regeln und Prozeduren muss von allen verstanden werden.
- **Mentale Modelle**
  Die sicherheitsrelevanten Bilder, Vorstellungen und Erwartungen müssen von allen geteilt werden.

[6] Diese Darstellung ist orientiert an einem Webinar von Prof. Dr. Harald Schaub, IABG, mit dem Titel „Social Hacking – Psychologische Grundlagen des Social Engineering oder Warum Firewalls nichts nützen“ (2019).

- **Kommunikation**
  Alle Kommunikationskanäle und Kommunikationswege müssen die Ausbildung der Emotionen, Motivationen, Kognitionen und des Wissens unterstützen.

Die Gestaltung von Arbeitsabläufen trägt ebenfalls zur Sicherheitskultur bei. Hier kommt es darauf an, alles zu vermeiden, was die „Anfälligkeit" für nicht-sicherheitsgerichtetes Verhalten erhöht. Dazu gehören u. a. das Erfordernis permanenter Aufmerksamkeit, ermüdende Tätigkeiten, andauernde Monotonie, seltene Ereignisse, zusammenhanglose Kommunikation und als sinnlos empfundene Aktivitäten. Vielmehr sollten bei den Mitarbeitern solche Stärken gefördert werden, die auch der Sicherheitskultur und dem Sicherheitsbewusstsein zugutekommen, wie Kreativität, Problemlösungsorientierung, Neugierde, Intuition, Verantwortungsgefühl, gemeinsame Werte und Ethik.

5 Methoden und Techniken im Überblick

Im Bereich Schulung und Sensibilisierung werden Begriffe nicht immer einheitlich und klar voneinander abgegrenzt verwendet. Daher wird hier zunächst ein Überblick über allgemein gängige Formate und ihre Bezeichnungen gegeben. Anschließend kurz wird auf einzelne Aspekte von Schulungen bzw. Schulungsveranstaltungen und ihre jeweiligen Vor- und Nachteile im Hinblick auf Durchführung und Wirkung eingegangen. Die zugehörigen Kommentierungen sind weitgehend allgemeingültig, also nicht nur auf die Zielgruppe „Management" beschränkt.

5.1.1 Unterschiedliche Formate und Bezeichnungen

Training
In einem Training wird etwas trainiert: Die Teilnehmenden üben etwas und verbessern ihre Fähigkeiten. Der Begriff ist international gebräuchlich und wird auch im Sport verwendet. Im Bereich der Weiterbildung wird „Training" häufig gleichbedeutend mit „Seminar" verwendet.

Seminar
Seminare werden an Universitäten und anderen Bildungseinrichtungen gehalten, von einem Dozenten geleitet, und haben dort i. d. R. theoretisch-wissenschaftliche Themen zum Inhalt. Neben referierenden Anteilen können sich die Teilnehmer in mehr oder weniger freier Diskussion zum jeweiligen Thema austauschen. Auch im Bereich der Weiterbildung ist „Seminar" – in vergleichbarer Bedeutung – ein etablierter Begriff.

Schulung
Schulung allgemein bedeutet das organisierte Vermitteln von Inhalten. Im vorliegenden Dokument wird „Schulungsveranstaltung" in diesem allgemeinen Sinn verwendet.
In einer Schulung, als einzelne „Veranstaltung" verstanden, werden die Inhalte i. d. R. frontal vermittelt. Eine Schulung folgt einem festgelegten Ablauf und ist insofern standardisierter als ein Seminar.

Lehrgang / Kurs
Die Begriffe „Lehrgang“ und „Kurs“ werden häufig gleichbedeutend verwendet. Ein Lehrgang besteht aus mehreren jeweils als Seminar oder Schulung gestalteten Abschnitten (auch als Module bezeichnet), die in größerem zeitlichen Abstand stattfinden. Lehrgänge oder Kurse werden sowohl als Präsenzveranstaltungen als auch über digitale Medien angeboten und können auch „gemischt“ organisiert sein, z. B. als Online-Kurs mit jeweils einem Präsenz-Modul zu Beginn und Abschluss. Siehe hierzu auch unten zum Begriff „Blended Learning“.

Workshop
Im Vergleich zum Seminar handelt es sich beim Workshop eher um ein Arbeitstreffen, bei dem Inhalte bzw. Lernziele und Ablauf weniger stark im Voraus festgelegt sind. Ein Workshop wird meist von einem oder mehreren Moderatoren geleitet, die den Gruppenprozess steuern und für die Ergebnissicherung sorgen.

Präsentation oder Vortrag
Diese Begriffe werden sowohl für eine Methode verwendet, die in einem Seminar oder Workshop eingesetzt werden kann, als auch für alleinstehende Veranstaltungen. In beiden Fällen gibt es einen Vortragenden, der den jeweiligen Inhalt mehr oder weniger „frontal“ an die Teilnehmer vermittelt, häufig ergänzt durch eine anschließende Gelegenheit für die Teilnehmer, Fragen zu stellen bzw. eine Diskussion zu führen.

Blended Learning
Unter „Blended Learning“, auch als „integriertes Lernen“ bezeichnet, wird eine Mischung aus Präsenz- und Online-Phasen in einem Kurs oder Lehrgang verstanden, die mit dem Ziel eingesetzt werden, deren jeweilige Vorteile zu verstärken und Nachteile zu kompensieren.
Als Vorteile einer Präsenzveranstaltung gelten vor allem die Möglichkeiten zu sozialem Kontakt, ganzheitlicher Kommunikation und flexiblen Reaktionen. Organisatorische Nachteile entstehen daraus, dass die Teilnehmer am gleichen Ort sein müssen und ähnliches Vorwissen mitbringen sollten. Das Lerntempo ist kaum individualisierbar.
Vorteile des E-Learning liegen in der zeitlichen und räumlichen Flexibilität, die den Teilnehmern ein individuelles Lerntempo ermöglicht, und der Möglichkeit zur individuellen Betreuung. Nachteile liegen in der schwerer herzustellenden sozialen Bindung und einer ggf. nicht ausreichenden Selbstlernkompetenz der Teilnehmer.

Webinar
Ein Webinar ist ein „live“ stattfindendes Seminar, das in Echtzeit per Internetverbindung an die Teilnehmer übertragen wird, wobei geeignete Visualisierungen eingebunden werden können. Über eine Chat-Funktion können die Teilnehmer mit dem Dozenten kommunizieren.

5.1.2 Einzelne Aspekte von Schulungsveranstaltungen: Vor- und Nachteile

Im Rahmen dieses Arbeitsschrittes AS 12.2.17 wurde die folgende Übersicht unter Einbeziehung eigener Schulungserfahrungen der beteiligten Konsortialpartner erarbeitet. Sie zeigt zu einzelnen Aspekten von Schulungsveranstaltungen deren mögliche Vor- und Nachteile auf,

die bei der Planung solcher Veranstaltungen bedacht und ggf. berücksichtigt werden sollten. Ergänzend enthält die Übersicht einige Hinweise zur Eignung von Veranstaltungen mit bestimmten Eigenschaften für bestimmte Zwecke sowie zu weiteren relevanten Einflussfaktoren, die sich bei der Durchführung auswirken können.

- Größe bzw. Anzahl der Teilnehmer,
- Zeitlicher Rahmen,
- Häufigkeit / Wiederholung,
- Art der Darstellung,
- Grad der Verallgemeinerung von Inhalten,
- Thematisierung von Gefährdungen und Risiken,
- Bewertung von Kenntnissen und Verhaltensweisen der Mitarbeiter.

Die Übersicht ist bewusst kurz gehalten und soll hier nur einer allgemeinen Orientierung dienen. Zur weiteren Vertiefung wird auf die entsprechende Fachliteratur verwiesen.

Veranstaltung: Form / Inhalt	**Wirkungen**		**Bemerkungen**
	günstig / motivierend	**ungünstig / demotivierend**	
Größe bzw. Anzahl Teilnehmer			
Große Gruppe	Aktivierend: Gemeinsamkeit, vielfältige Anregungen und Möglichkeiten zum Austausch, „Vernetzung“.	Deaktivierend: Keine „Blöße geben“, in großer Runde keine Fragen stellen.	Gut geeignet für allgemeine Themen, Information.
Kleine Gruppe	Mehr Möglichkeit zu individueller Unterstützung, „persönlichere“ Atmosphäre.	Bei ungünstiger Kombination der Teilnehmer gibt es evtl. eine starke emotional „überlagernde“ Wirkung.	Gut geeignet für individuelles Lernen, Coaching.
Einzeltraining[7] (ggf. individuell angepasst, aber kein Coaching)	Besonders günstige Aufnahmevoraussetzungen durch Anpassung an eigene Interessen und eigenes Lerntempo.	Individuelle Wahrnehmungen und Bewertungen bleiben ggf. ohne Rückmeldung oder Relativierung.	Sehr flexibel einsetzbar.

[7] Im Unterschied zum Einzeltraining, das z. B. auf Basis von Online-Angeboten erfolgen kann, ist das Coaching in jeder Hinsicht individuell anpassbar, allerdings auch mit dem entsprechend hohen finanziellen, personellen und zeitlichen Aufwand verbunden.

Veranstaltung: Form / Inhalt	Wirkungen		Bemerkungen
	günstig / motivierend	ungünstig / demotivierend	
Zeitlicher Rahmen			
Kurzveranstaltung (<= 30 Min.)	Leicht einzuplanen, als wenig „störend“ im allg. Arbeitsablauf empfunden.	Themen können evtl. nicht hinreichend vertieft werden, auf Anliegen / Fragen der Teilnehmer kann nicht ausreichend eingegangen werden.	
Mittlere Dauer der Lektion / Trainingseinheit (1 bis 2 Stunden)	Relativ leicht einplanbar, die Aufmerksamkeit der Teilnehmer wird nicht überfordert.		
Lange Dauer der Lektion / Trainingseinheit / Veranstaltung (halb- bzw. ganztägig oder mehrtägig)	Themen können vertieft und vielseitig behandelt werden, Theorie und Praxis können sich ergänzen, auf Anliegen und Rückmeldungen der Teilnehmer wird eingegangen.	Termin kann weniger leicht eingeplant werden, Teilnehmer sind evtl. stärker abgelenkt durch Aufgaben und Verpflichtungen außerhalb der Veranstaltung.	
Häufigkeit / Wiederholung			
Regelmäßige Wiederholung allgemein relevanter Schulungen	„Auffrischung“, die Vertrautheit mit den Themen wird vertieft, Verhaltensweisen werden verankert.	Möglicher „Abstumpfungseffekt“ beeinträchtigt die Aufmerksamkeit.	Wiederholungen sollten möglichst auch neuen – oder zumindest variierten – Inhalt anbieten.
Häufige kurze Schulungen	Die Thematik insgesamt bleibt präsent, auf aktuelle Themen kann kurzfristig eingegangen werden.	Wegen fehlender Vertiefung bleibt die Wirkung zu komplexeren Themen evtl. oberflächlich.	

Veranstaltung: Form / Inhalt	Wirkungen		Bemerkungen
	günstig / motivierend	ungünstig / demotivierend	
Seltene lange Schulungen	Zusammenhängende und vertiefte Beschäftigung mit Themen wirkt nachhaltig.	Thematik bleibt in den Zwischenzeiten nicht präsent, auf aktuelle Themen kann nur mit Verzug eingegangen werden.	
Art der Darstellung			
Präsentation durch **professionelle Moderatoren**	Professioneller Eindruck, überzeugend, „gewohnt“, kann leicht aufgenommen werden.	Evtl. zu „glatt“, kann eine passive Aufnahme-Haltung verstärken, erzeugt keine persönliche Betroffenheit.	
Beitrag von **realen Rollenträgern / Betroffenen**	Authentischer Eindruck, überzeugend, motivierend.	Evtl. einseitige, persönliche Wahrnehmung, didaktische Schwächen, nicht ausreichend zielgruppengerecht aufbereitet. Falls zu intensiv: ängstigend, demotivierend.	
Grad der Verallgemeinerung von Inhalten			
Allgemeine Information	Überblick, Zusammenhänge, Hintergrund.	Kein Hineinversetzen/ „Miterleben“ von konkreten Situationen/Angriffen/Schäden	
Konkretes Fallbeispiel	Authentisch, plausibel, veranschaulicht und macht betroffen, kann individuell passend ausgewählt werden.	Verharmlosung als „Einzelfall“ oder Ausnahme ermöglicht Distanzierung.	
Thematisierung von Gefährdungen und Risiken			

Veranstaltung: Form / Inhalt	Wirkungen		Bemerkungen
	günstig / motivierend	ungünstig / demotivierend	
Betont sachliche Darstellung von Gefährdungen und Risiken	Professioneller Eindruck, erzeugt keine Abwehr.	Evtl. zu neutral, erzeugt keinen Bezug zur eigenen Situation.	
Eindringliche Darstellung konkreter Risiken und Folgen	Erhöht das Risikobewusstsein, überzeugt, macht betroffen.	Kann Angst und somit – ggf. auch unbewusste – Abwehr erzeugen.	
Bewertung von Kenntnissen und Verhaltensweisen der Mitarbeiter			
Sichtbare Bewertung von Kenntnissen in Gruppe / Team	Erfolgserlebnisse erhöhen die Motivation.	Misserfolg kann demotivierend wirken.	Lösung vorgegebener Aufgaben in (konkurrierenden) Teams „schützt“ einzelne Teilnehmer
Individuelle Bewertung von Kenntnissen	Erfolgserlebnisse erhöhen die Motivation, auch Misserfolg kann anspornend wirken.	Misserfolg kann demotivierend wirken.	Wenn vom Lernerfolg etwas anderes abhängt (Zertifikat etc.), kann dies kurzfristig motivierend wirken.
Sichtbare Bewertung von Verhaltensweisen vor Kollegen, Mitarbeitern	Engagement, Sorgfalt, Konsequenz etc. können durch soziale Anerkennung verstärkt werden.	Erwünschte Verhaltensweisen können durch zu starke Betonung als übertrieben, kleinkariert, paranoid empfunden werden, was zu Ablehnung führt.	Die Unternehmenskultur hat wesentlichen Einfluss auf Bewusstsein und Verhalten der Mitarbeiter.
Individuelle Bewertung im Einzelgespräch	Engagement, Sorgfalt, Konsequenz etc. können durch Anerkennung verstärkt werden, zu Defiziten können Optionen aufgezeigt	Der Eindruck einer zu starken „Überwachung“ kann demotivierend wirken.	Die entsprechenden Voraussetzungen müssen in der Unternehmenskultur gegeben sein:

Veranstaltung: Form / Inhalt	Wirkungen		Bemerkungen
	günstig / motivierend	ungünstig / demotivierend	
	werden, Mitarbeiter-Feedback ist möglich.		Offenheit, Vertraulichkeit, ggf. anonyme Meldewege.

Tabelle 1: Einzelne Aspekte von Schulungsveranstaltungen: Vor- und Nachteile

5.1.3 Der besondere Stellenwert der Gamification

In den Berichten, Diskussionen und Beispielen zum Thema Schulung und Sensibilisierung im Arbeitsschritt 12.2.17 wurde immer wieder hervorgehoben, wie wichtig es ist – und dies gilt für *alle* Zielgruppen –, die relevanten Informationen zum Thema Informationssicherheit und die zugehörigen Verhaltensweisen in einer Weise zu vermitteln, die zur Teilnahme und Auseinandersetzung motiviert, die Informationsaufnahme und Lernerfolg positiv verstärkt und die möglichst den Wunsch nach Wiederholung weckt.

Vor diesem Hintergrund wurde der Stellenwert der sog. „Gamification" deutlich – siehe hierzu auch die Mehrzahl der im folgenden Kapitel 6 vorgestellten Beispiele. Laut Gabler Wirtschaftslexikon ist Gamification[8] die Übertragung von spieltypischen Elementen und Vorgängen in spielfremde Zusammenhänge. „Zu diesen spieltypischen Elementen gehören unter anderem Erfahrungspunkte, Highscores, Fortschrittsbalken, Ranglisten, virtuelle Güter oder Auszeichnungen. Durch die Integration dieser spielerischen Elemente soll im Wesentlichen eine Motivationssteigerung der Personen erreicht werden, die ansonsten wenig herausfordernde, als zu monoton empfundene oder zu komplexe Aufgaben erfüllen müssen." [9]

Auch wenn von Fachleuten die Themen der Informationssicherheit sicherlich als Herausforderungen angesehen werden, die keineswegs als monoton bezeichnet werden können, so ist doch immer wieder zu beobachten, dass die übrigen Angehörigen eines Unternehmens sich vielfach nicht gerne mit Sicherheitsthemen befassen, sei es mangels empfundener eigener Betroffenheit oder auch aufgrund von Berührungsängsten mit einer als tendenziell trocken, kompliziert, unerfreulich, vielleicht sogar als bedrohlich wahrgenommenen Thematik. Und solange nichts „passiert", wird auch der Stellenwert des Themas leicht als relativ gering eingeschätzt gegenüber den Herausforderungen des Tagesgeschäfts. Motivation muss also mit anderen Mitteln erzeugt werden, wobei Gamification sich als wirksamer Faktor erweist. Im Folgenden werden die wichtigsten Prinzipien der Gamification kurz vorgestellt.[10]

Spiel[11] **(**Game)

Allgemein sind bei einem Spiel diese Aspekte wesentlich:

- Spaß: Die Aktivität wird wegen ihres unbeschwerten Charakters gewählt.
- Ereignis: Die Aktivität ist räumlich und zeitlich begrenzt.
- Ungewiss: Ablauf und Ergebnis der Aktivität sind offen bzw. nicht vorhersehbar.
- Unproduktiv: Die Teilnahme bewirkt nichts Nützliches im Sinne einer realen Dienstleistung.
- Regelbasiert: Die Aktivität folgt Regeln, die sich allerdings von denen des Alltagslebens unterscheiden.
- Fiktiv: Man lebt während des Spiels in einer „anderen" Realität.

---

[8] Alternative Begriffe im deutschsprachigen Raum sind "Gamifizierung" und "Spielifizierung". Siehe https://wirtschaftslexikon.gabler.de/definition/gamification-53874

[9] Siehe: https://de.wikipedia.org/wiki/Gamification

[10] Die Darstellung ist orientiert an einem Vortrag von Prof. Dr. Harald Schaub, IABG, bei der Concept Development & Experimentation (CD&E) Conference, 2015, Berlin.

[11] Charakteristika nach Roger Callois, frz. Soziologe.

Lernspiel (Educational Game)

Lernspiele im engeren Sinne werden ausdrücklich zum Zweck des Lernens bzw. der Ausbildung entworfen bzw. sie haben eine solche Nebenwirkung. In einer Lernumgebung können alle Arten von Spielen eingesetzt werden.

Lernspiele helfen beim Lernen bezogen auf

- Spezielle Themen,
- Erweiterung von Themenfeldern bzw. Konzepten,
- Verstärkung von Entwicklungen,
- Verständnis historischer oder fremder Ereignisse und Kulturen,
- Spielerisches Erlernen einer Fähigkeit.

Ernsthaftes Spiel (Serious Game)

Bei der Gamification werden Denkweise und Ablaufregeln von Spielen in einem nicht-spielerischen Kontext eingesetzt, um Schüler, Studenten oder Mitarbeiter eines Unternehmens zu einem Lernprozess zu motivieren. Dabei besteht das Ziel darin, durch Freude und Engagement beim Lernen das Interesse der Lernenden zu wecken und sie dadurch zum Weiterlernen zu inspirieren. Das geschieht u. a. durch diese angestrebten Wirkungen der Gamification:

- Selbständigkeit beim Lernen,
- Entwicklung der eigenen Individualität durch unterschiedliche Rollen,
- Gelegenheit zu Versuch und Irrtum ohne negative Konsequenzen,
- Mehr Spaß und Freude im Unterricht,
- Möglichkeit zu individuellem Lernen,
- Sichtbare Lernerfolge,
- Förderung der intrinsischen Motivation zum Lernen.

Entsprechend ihrer Zielsetzung werden solche Spiele auch als **Serious Games** (englisch für *ernsthafte Spiele*) bezeichnet. Darunter versteht man „digitale Spiele, die nicht primär oder ausschließlich der Unterhaltung dienen, wohl aber derartige Elemente enthalten können. Gemein haben Serious Games – wie auch Lernspiele – das Anliegen, Information und Bildung zu vermitteln“[12].

Beispiele für solche Serious Games finden sich im folgenden Kapitel, siehe „Escape Game / Escape Room“ (Kapitel 6.1), „Point-and-Click-Adventure“ (Kapitel 6.2) und „Game of Threats™“ (Kapitel 6.3).

[12] Siehe Wikipedia: https://de.wikipedia.org/wiki/Serious_Game

6 Schulung und Sensibilisierung zur Informationssicherheit: Beispiele

Die in den folgenden Unterkapiteln in unterschiedlicher Ausführlichkeit vorgestellten Schulungsformate wurden vor allem ausgewählt, weil sie von den üblichen Seminaren, Schulungen und Trainings insofern abweichen, als ungewohnte, unkonventionelle oder aufwendige Methoden und Techniken eingesetzt werden, um zur Teilnahme und Mitarbeit zu motivieren und den jeweiligen Schulungs- und Sensibilisierungs-Erfolg zu verbessern. Sie sind insofern für die nicht immer leicht für zu motivierende Zielgruppe „Management“ vielfach gut geeignet. Die auf der enera-Lernplattform angebotenen Trainings zum Thema Informationssicherheit werden hier ebenfalls beschrieben.

Einige der Beispiele wurden von enera-Konsortialpartnern entwickelt und z. T. bereits eingesetzt, die übrigen basieren weitgehend auf Erfahrungsberichten der beteiligten Konsortialpartner im AS 12.2.17.

6.1 Escape Game / Escape Room

6.1.1 Format

Escape Games oder Escape Room Games gehören zum Genre der Adventure Games. Sie werden meist als Computerspiele angeboten, können jedoch auch „real“ inszeniert werden. Das Ziel des Spiels besteht darin, einen Ort, an dem man gefangen ist, zu verlassen. Meist agiert der Spieler als Einzelspieler, und er kann sich nur durch Geduld, Ausdauer, Geschicklichkeit und logisches Denken / „Kombinieren“ befreien.

6.1.2 Beispiel „Escape Room“ (EWE)

Bei EWE Netz wurde ein neuartiges Schulungsformat zur Erhöhung der Security Awareness unter dem Namen „Escape Room“ entwickelt und mit Erfolg eingesetzt.

„Escape Room“ ist ein Rätselspiel, dessen Ziel es ist, sich in einem festgelegten Zeitrahmen durch die Lösung verschiedener expliziter und impliziter Herausforderungen aus einer vorgegebenen Problemlage bzw. Aufgabenstellung zu „befreien“.

Zielgruppe waren bisher Führungskräfte, die Schulung ist aber auch bei anderen Zielgruppen einsetzbar. In der kurzen und motivierenden Präsenzschulung bewirkte die spielerische Aufarbeitung von Alltagsproblemen mit Sicherheitsbezug eine Erhöhung der Wahrnehmung von Sicherheitsaspekten. Der realitätsnahe Themenbezug sorgt für sofortige Lerneffekte.

Im Vergleich zu e-Learnings wurde ein deutlich erhöhter Lerneffekt beobachtet. Der erforderliche Aufwand für die Vorbereitung und Durchführung des Schulungsformates wurde als relativ gering bewertet.

Zu weiteren Einzelheiten siehe Anlage 1 zu diesem Dokument.

6.2 Point-and-Click-Adventure

6.2.1 Format

Point-and-Click (Englisch für: auf etwas zeigen und [es] anklicken) ist ein Konzept für die Interaktion mit Computerprogrammen, wobei durch das Positionieren des Cursors und anschließendes Bedienen einer Taste des Eingabegeräts eine vordefinierte Aktion ausgelöst wird. Dieses Prinzip wird in der gleich benannten Art von Computerspielen genutzt. Z. B. kann es erforderlich sein, dass ein Spieler in einem Raum befindliche Objekte mit der Computermaus zunächst anvisiert (= Point) und dann anklickt (= Click), um mit diesen Objekten zu interagieren.

Adventure-Spiele sind ein Genre von Computerspielen, bei denen durch Erkundung und das Lösen von Rätseln eine dem Spiel zugrunde liegende Geschichte erlebt wird. Ein elementarer Bestandteil von Point-and-Click-Adventures ist entsprechend das Verknüpfen von Gegenständen und Objekten, um neue Objekte und Hinweise zu bekommen. Dabei müssen auch die Hinweise richtig interpretiert oder Rätsel gelöst werden, um – z. B. in der Ausprägung „Escape Room“ (siehe auch Kapitel 6.1) – an erforderliche Codes oder Passwörter zu gelangen.

6.2.2 Beispiel Point-And-Click-Adventure (OFFIS, noch unbenannt)

Hinweis: *Aktuell (Oktober 2020) befindet sich das Spiel noch im Entwicklungsstadium.*

Beim OFFIS wurde ein Computerspiel zur Sensibilisierung für Informationssicherheit entwickelt. Das Spiel ist dabei als Point-And-Click-Adventure umgesetzt, bei dem der Spieler eingebaute Sicherheitslücken ausnutzen muss, um in der Geschichte voran zu kommen.

Der Spieler nimmt die Rolle eines Charakters ein, der die Machenschaften einer kriminellen Gruppe unterbinden möchte, indem er Informationen über die kriminelle Gruppe ausspioniert und ihre Abwehrmaßnahmen aushebelt, um ihren Standort aufzudecken und das kriminelle Geschäft zu beenden. Die im Spiel eingebauten Sicherheitslücken entsprechen dabei den Inhalten, die zur Sensibilisierung adressiert werden sollen. So kann beispielsweise ein Rätsel gelöst werden, indem der ungeschützte Rechner z. B. in der Mittagspause ausgenutzt wird, Einsicht in herumliegende Dokumente genommen wird oder auch USB Sticks mit Schadsoftware verteilt werden, um damit dann Zugang zu einem der Rechner der kriminellen Gruppe zu erlangen.

Die Zielgruppe für das Spiel sind Mitarbeiter (allgemein), da durch das Spiel eine große Gruppe von Personen zu individuellen Zeiten erreicht werden kann. Das Spiel gliedert sich in mehrere Etappen und kann jederzeit gespeichert werden, sodass es Teilziele zum Erreichen gibt und das Spiel auch jederzeit unterbrochen werden kann. Durch die spielerische Gestaltung wird eine große Motivation zur Teilnahme erhofft. Der Lerneffekt soll dadurch erhöht werden, dass beim Laden des Spiels Sicherheitshinweise wie „Sperre immer deinen Rechner, wenn du das Büro verlässt“ eingeblendet werden. Des Weiteren ist im Spiel beim Abschluss einzelner Etappen der Geschichte eine Zwischensequenz eingebaut, bei der durch einen Dialog mit einem anderen Charakter darauf hingewiesen wird, dass die soeben ausgenutzte Sicherheitslücke auch im eigenen Berufsalltag auftreten und negative Folgen haben kann.

6.3 Game of Threats™ – Cyber Security-Simulation für Manager

6.3.1 Format

Das Simulationsspiel „Game of Threats™“ des Beratungsunternehmens PWC wird von den Teilnehmern mit Computer-Unterstützung und unter Begleitung von Moderatoren in Teams durchgeführt und dauert i. d. R. weniger als eine Stunde. PWC beschreibt das Spiel so[13]:

> Game of Threats™ ist eine Simulation, die der Managementebene eines Unternehmens das Verständnis für den Ablauf und die Dynamik von Cyberangriffen “hautnah“ vermitteln kann. Das Spiel greift dabei Elemente der Gamifizierung genauso wie Aspekte der Spieltheorie auf – und schafft für den Nutzer ein in dieser Form neuartiges interaktives Erlebnis. Konkret geht es bei Game of Threats™ darum, dass das „Team Unternehmen“ die eigene Firma gegen das „Team Angriff“ verteidigen muss. Das Spiel mutiert dabei zu einer realen Erfahrung, bei der beide Seiten gefordert sind, in kürzester Zeit existenzielle Entscheidungen zu treffen – und das auf Basis begrenzter Informationen und knapper finanzieller Ressourcen. Für richtige Entscheidungen werden die Spieler belohnt, für schlechte bestraft.
>
> Die Manager eines Unternehmens werden bei Game of Threats™ auf beide Teams aufgeteilt. Das zwingt sie, sich nicht nur mit der eigenen Perspektive, sondern auch mit der des Angreifers auseinanderzusetzen. Während die eine Mannschaft den nächsten Angriff plant, muss das andere die passende Abwehrmaßnahme entwickeln. Die Moderatoren von PWC geben den Spielern dabei laufend Feedback, ob ihre Entscheidungen in die richtige Richtung führen – und welche alternativen Strategien es womöglich gibt. Am Ende geht es darum, dass das Management durch Game of Threats™ ein besseres Verständnis für den Umgang mit der Cyber-Bedrohung erhält.“

6.3.2 Beispiel Game of Threats auf einer Messe

Bei der AFCEA Fachausstellung 2019[14] in Bonn wurde das Game of Threats™ in einem separaten Großraum frei zur Teilnahme angeboten und stieß auf so viel Interesse, dass Teilnehmer zeitweise erst nach einer gewissen Wartezeit einen Platz in einem der Teams (Angreifer bzw. Verteidiger) erhielten. Jede der beiden Gruppen (ca. 5 Teilnehmer) versammelte sich jeweils vor einem großen Bildschirm, auf dem aus einem umfangreichen Arsenal an Maßnahmen zum Angriff auf das gegnerische bzw. zur Verteidigung des fiktiven eigenen Unternehmens ausgewählt werden konnten. Jedes Team verfügte nur über ein begrenztes Budget für

[13] Siehe https://www.pwc.de/de/digitale-transformation/game-of-threats-cybersecurity-simulation-fuer-manager.html.

[14] Siehe https://www.afcea.de/veranstaltungen/fachausstellung/fachausstellung-2019/ausstellung-2019.html.

die „kostenpflichtig“ angebotenen Methoden und Techniken – daher war eine sorgfältige Auswahl erforderlich, welche Mittel in der gegebenen Situation überhaupt angemessen und am wirksamsten sein würden. Da sie mit einer konkret simulierten Angriffs-Lage konfrontiert waren, bekamen die unterschiedlichen Optionen zur Abwehr für die Teilnehmer eine wesentlich konkretere Bedeutung, als es bei Lektüre oder Vortrag der Fall gewesen wäre, z. B.: Ein vergleichbares Unternehmen wurde bereits durch Malware angegriffen und erpresst – was könnte uns schützen? Oder: Die Verschlüsselung aller Nachrichten hat nicht gewirkt – was sonst könnte jetzt noch helfen? Nachdem pro Runde beide Gruppen ihre jeweiligen Entscheidungen eingegeben hatten, wurde in der Simulation angezeigt, wie wirksam die ausgewählten Methoden zu Angriff und Verteidigung gewesen waren, verbunden mit der Vergabe von Punkten, so dass der Punktestand nach der letzten derartigen Runde über Gewinner und Verlierer entschied.

Da es sich um ein unspezifisches fiktives Unternehmen handelte, konnten auf diese Weise nur grundsätzliche Informationen vermittelt werden – dies geschah durch den Spielcharakter durchaus motivierend und anschaulich. Eine solche Simulation wäre also für einen ersten Einstieg in die Thematik gut geeignet. Anpassungen auf spezifische Branchen / Unternehmen wären nur mit beachtlichem Aufwand möglich, ebenso eine Aktualisierung entsprechend dem technischen Fortschritt auf Angreifer- und Verteidiger-Seite. Die Gruppen waren zufällig gemischt, wobei sich schnell „Wortführer“ hervortaten, was zur relativen Passivität weiterer Gruppenmitglieder führte – die intensive Betreuung durch erfahrene Moderatoren erscheint daher wesentlich.

6.4 Cyber Range

6.4.1 Format

Als Cyber Ranges werden kontrollierte virtuelle Umgebungen bezeichnet, in denen Randbedingungen und Durchführung von Cyber-Angriffen und -Verteidigung simuliert werden, wobei Durchführung und Ergebnisse wiederholt und optimiert werden können. Es handelt sich dabei um komplexe Plattformen, die für den jeweiligen Simulations- bzw. Trainingszweck angepasst werden.

6.4.2 Beispiel „CyberRange-e: Cybersecurity für Stromnetze“

Das Unternehmen Innogy SE bietet mehrtägige Trainings zur Cybersicherheit im eigenen Trainingszentrum an, Zielgruppe sind Energieversorger und Netzbetreiber.

Angeboten werden

- Vorbereitung mit Nachbildung der Kunden IT / OT-Infrastruktur,
- Training als War Gaming (Blue Team, Red Team, White Team = Coaches)
- Trainings-Teilnahme im Blue Team in der gewohnten Rolle (z. B. Betriebspersonal, Management)

Der Anbieter schreibt hierzu[15]:“Hier können Sie als Energieversorger und Netzbetreiber testen, ob Ihre Notfallprozesse effektiv und effizient funktionieren – ohne Ihr eigenes System einer echten Gefahr auszusetzen. Das Training hilft Ihnen dabei, Ihre Widerstandsfähigkeit im Netzbetrieb zu erhöhen und die Abwehr eines Cyberangriffs einzuüben.“

[15] Siehe https://news.innogy.com/energieversorger-lernen-abwehr-von-hackerangriffen/ sowie bei der Tochtergesellschaft innogy Westenergie GmbH: https://www.westenergie.de/unternehmen/netzservice/produkte/cyberrange-e

6.5 Rollenspiel (Simulation)

6.5.1 Format

Ein Rollenspiel kann zur Simulation eines Gesprächs oder Konfliktes zwischen zwei oder mehr Personen eingesetzt werden, um eine Erfahrung davon zu vermitteln, wie eine schwierige Situation erlebt wird und welches Verhalten darin welche Wirkungen hervorrufen kann[16].

Die Teilnehmer erhalten vor Beginn des Rollenspiels Informationen zur Situation und ihrer eigenen Rollen darin. Günstig im Kontext von Schulung und Sensibilisierung zu Sicherheitsthemen ist die Durchführung vor einer Gruppe von Kollegen (die das Spiel, evtl. abgewandelt, ebenfalls durchführen können) und in Anwesenheit eines erfahrenen Trainers. Wesentlich ist, dass nach Durchführung des Spiels sowohl die Perspektive der unmittelbaren Teilnehmer zur Sprache kommt als auch die Wahrnehmung der teilnehmenden Zuschauer. Im anschließenden moderierten Austausch zum Verlauf des Rollenspiels (Wie fühlten sich die Teilnehmer, was war einfach, was war schwierig, welche Alternativen hätte es gegeben, usw.) kann die Erfahrung aufgearbeitet und vertieft werden. Durch das unmittelbare Erleben ist eine nachhaltigere Sensibilisierung und ggf. Verhaltensänderung zu erwarten, als durch die rein passive Aufnahme von Inhalten.

Geeignete Themen für Rollenspiele finden sich im Bereich der persönlichen, „alltäglichen“ Erfahrung der Teilnehmer, z. B.

- Umgang mit unbekannten Personen auf dem Unternehmensgelände,
- Umgang mit Aufforderungen zu unzulässigem Verhalten,
- Vorgehen im Anschluss an oder als Reaktion auf eigenes oder fremdes Fehlverhalten

Vorschläge für konkrete Rollenspiele zu solchen Themen enthält das folgende Unterkapitel 6.5.2. Bedingt durch die Verlagerung der in 2020 als Präsenztreffen vorgesehenen AP12-Arbeitstreffen in den virtuellen Raum konnten Rollenspiele zu diesen Themen leider nicht – wie ursprünglich geplant – live erprobt und bewertet werden.

Ergänzend wird im Unterkapitel 6.5.3 das „Social Hacking“ aus dem Themenfeld „Social Engineering“ ausführlich betrachtet, da es viele weitere mögliche Themen für Rollenspiele beinhaltet.

Die Vorgehensweise zur Durchführung des Rollenspiels in einer Gruppe von Mitarbeitern umfasst typischerweise die folgenden Schritte. Wichtig ist hierbei immer die Leitung durch einen professionellen und erfahrenen Moderator.

- Kurzer Überblick über den Verlauf, Aufforderung an freiwillige Teilnehmer.
- Individuelle Vorbereitung der Teilnehmer auf Basis einiger Stichworte zu ihrer Rolle und Aufgabe, die sie jeweils auf einer „Rollenkarte“ erhalten.

[16] Einen allgemeinen Überblick über Methodik und Funktionsweise des Rollenspiels gibt z. B. diese kurze Einführung in die Thematik aus dem Bereich „Unterrichtsmethoden im konstruktiven und systemischen Methodenpool“ der Universität Köln (o. A. zum Verfasser): http://methodenpool.uni-koeln.de/download/rollenspiele.pdf

- Die Teilnehmer spielen die Szene in ihrer jeweiligen Rolle, evtl. unterstützt durch den Moderator. Eine Zeitdauer von wenigen Minuten kann schon ausreichen, sie sollte aber nicht von vornherein begrenzt sein.
- Abfrage bei den Zuschauern durch den Moderator, wie sie das Rollenspiel erlebt haben.
- Abfrage bei den Teilnehmern selbst, wie sie das Rollenspiel erlebt haben.
- Weitere Erörterung von bei der Abfrage aufgekommenen Themen und Fragestellungen in einer moderierten Gruppen-Diskussion.

Im Anschluss kann ggf. ein weiteres Rollenspiel mit einem anderen, aber möglichst verwandten, Thema durchgeführt werden – bei Teilnehmerinteresse natürlich auch mit dem gleichen Thema – sofern die verfügbare Zeit ausreicht.

Bei allen Rollenspielen ist es wichtig, den Kontext der Unternehmenskultur zu beachten, da sie immer „mitspielt“: Nicht nur von Bewusstsein und Verhalten des einzelnen Mitarbeiters hängen Erfolg oder Misserfolg der Sensibilisierung durch ein Rollenspiel ab, sondern auch davon, welchen allgemeinen Stellenwert Problembewusstsein und Offenheit im Unternehmen haben (siehe hierzu auch Kapitel 4.4).

6.5.2 Themenvorschläge für konkrete Rollenspiele

Einige der folgenden Themen werden in verschiedenen Unternehmen und Organisationen u. a. in Mitarbeiter-Broschüren, Plakaten und Merkblättern zum Thema Informationssicherheit angesprochen, einige weitere entstammen persönlichen Erfahrungen der Projektbeteiligten. Aus unserer Sicht sind sie gut geeignet als Ausgangspunkte für Rollenspiele, bei denen die Teilnehmer nicht nur abstrakt über ein Thema reflektieren, sondern erleben können, wie es sich tatsächlich „anfühlt“, in einer solchen Situation zu sein.

Die folgenden Beschreibungen enthalten Stichworte als Anregung für die eigene konkrete und vollständige Ausgestaltung.

6.5.2.1 Sicherheit vor Höflichkeit

Es geht darum, wie man sich als Mitarbeiter fühlt, wenn man sich aus Gründen der (Informations-)Sicherheit gezwungen sieht, so bestimmt aufzutreten, dass es von Betroffenen als unhöflich und abweisend empfunden wird, und dabei evtl. die Verärgerung von Vorgesetzten oder Kollegen oder andere Folgeschäden riskiert. Die Spielerfahrung und anschließende Reflektion kann bei Vorgesetzten und Kollegen die Sensibilisierung und das Verständnis für die entsprechenden Sicherheitsregelungen und -maßnahmen und daraus resultierendes Verhalten stärken bzw. zu entsprechendem Verhalten ermutigen.

Spieler 1: Mitarbeiter am Empfang, Werkstor o. ä.

- Aufgabe: „Sorgen Sie als Empfangs-Mitarbeiter für die Einhaltung der geltenden Regeln“.

- Regel: Besucher und Lieferanten dürfen nur mit Firmenausweis eingelassen werden; andernfalls müssen sie warten, bis die Kontaktperson im Unternehmen den Besucher bzw. die Lieferung persönlich abholt.
- Randbedingung: Bereichsleiter x ist telefonisch nicht erreichbar

Spieler 2: Besucher, Lieferant (z. B. Pizza), Handwerker o. ä.

- Aufgabe: „Sie wollen Bereichsleiter x besuchen“ (bzw.: ihm etwas liefern).
  Sie haben es sehr eilig, da Sie sich zum Termin bereits verspätet haben (bzw. weil die Lieferung sehr eilig ist) und Schaden für sich bzw. das eigene Unternehmen befürchten, wenn Sie sich weiter verspäten.“
- Randbedingung: „Sie haben keinen Firmenausweis“

Varianten könnten z. B. Folgendes beinhalten

- Besucher ist ein Handwerker, der dringend etwas reparieren muss („wollen Sie für den sich verschlimmernden Wasserschaden verantwortlich sein?!?“) und sich lt. eigener Aussage gut im Gebäude auskennt.
- Mitarbeiter (nicht Pförtner) sieht unbekannte Person auf dem Gang / mit einem Arm voller Aktenordner vor der verschlossenen Tür zum Konferenzraum / mit einem USB-Stick am Drucker beschäftigt / beim Verlassen des Gebäudes vor dem Seiten-Ausgang, offenbar bestrebt, durch die gerade geöffnete Tür das Gebäude zu betreten.

6.5.2.2 Unsichere Medien

Es geht darum, wie man sich als Mitarbeiter fühlt, wenn man aus Gründen der Informationssicherheit ein Verhalten zeigen muss, das verständnislose Verärgerung bei Vorgesetzten oder Geschäftspartnern erzeugt. Die Spielerfahrung und anschließende Reflektion kann zu Überlegungen führen, welche geänderten Randbedingungen solche Situationen evtl. „entschärfen“ könnten, sowie zu einer Sensibilisierung für den sicheren Umgang mit „fremden“ Medien.

Spieler 1: Teilnehmer einer Besprechung im eigenen Unternehmen A mit einem Mitarbeiter des Unternehmens B, mit dem A bei einem anstehenden Projekt zusammenarbeiten / gemeinsam anbieten möchte.

- Aufgabe: „Klären Sie die folgenden Fragen (x, y,...) mit dem Mitarbeiter von B“.
  Das Projekt ist für unser Unternehmen von hohem Stellenwert, die Besprechung muss erfolgreich verlaufen.“
- Regel: Es dürfen keine unternehmensfremden Geräte / Medien / Datenträger ungeprüft Kontakt zu Unternehmensnetz oder -geräten haben.

Spieler 2: Mitarbeiter von Unternehmen B, Teilnehmer bei o. g. Besprechung

- Aufgabe: „Sie sind Experte für das Thema x (*entspricht der Frage x)* und möchten dazu anhand einer vorbereiteten Präsentation wesentliche Inhalte erläutern.“

- Randbedingung: Sie führen die Präsentation auf einem USB-Stick mit sich, verfügen aber über kein eigenes Gerät zur Vorführung und müssen daher Spieler 1 darum bitten, die Präsentation vom USB-Stick auf sein Vorführ-Gerät zu überspielen.

6.5.2.3 Soll ich das melden, und wenn ja, wie?

Es geht darum, allgemein für die Wahrnehmung von unter Sicherheitsaspekten problematischen Vorkommnissen und Verhaltensweisen zu sensibilisieren, sowie die ggf. erforderliche Kommunikation über solche Vorkommnisse zu erleichtern. Die Spielerfahrung und anschließende Reflektion kann einerseits zu Überlegungen führen, ob die vorhandenen Regelungen und Meldewege ausreichen – gibt es z. B. einen anonymen Briefkasten, sollte es ihn geben? – und andererseits ggf. zu angemessenem Verhalten ermutigen.

Spieler 1: Mitarbeiter im Unternehmen

- Situation: Sie waren mehrfach Zeuge, wie Kollege bzw. Kollegin x gegen Sicherheitsregelungen verstieß (realistisches Beispiel aus dem Unternehmensalltag, z. B. lässt vertrauliche Unterlagen oder Geräte offen herumliegen, telefoniert zu kritischen Themen in Anwesenheit von Besuchern, gibt vertrauliche Informationen an externe Projektkollegen weiter, usw. – das Beispiel könnte auch einer im Vorfeld entstandenen Themensammlung entnommen werden). Als Sie ihn bzw. sie darauf ansprachen, reagierte x verständnislos und bedrohlich, oder: Es handelt sich um einen Vorgesetzen, den Sie nicht direkt ansprechen wollen.
- Aufgabe: Informieren Sie eine dritte Person (z. B. ISB, Vorgesetzter, sonstige Vertrauensperson) über Ihre Beobachtungen, damit bei x eine Verhaltensänderung herbeigeführt werden kann. Fragen Sie nach dem weiteren Vorgehen.

Spieler 2: Mitarbeiter im gleichen Unternehmen (z. B. ISB, Vorgesetzter von Spieler 1, sonstige Vertrauensperson). Ggf. können ISB, Datenschutzbeauftragter etc auch in ihrer „eigenen“ Rolle teilnehmen.

- Situation: (Kurze Erläuterung der Rolle als ISB, Vorgesetzter, usw.)
- Aufgabe: Hören Sie an, was Spieler 1 Ihnen zu sagen hat. Setzen Sie ihn nicht unter Druck, streben Sie eine objektive Darstellung der Vorkommnisse an.

6.5.2.4 Sich selbst in die Rolle des „Täters“ versetzen

Es geht darum, die Vorstellungen davon, wie ein Angreifer vorgehen würde, zu konkretisieren, um Bewusstsein und Verständnis für die erforderlichen Schutzmaßnahmen zu stärken und für die Wahrnehmung von Schwachstellen zu sensibilisieren. Die Spielerfahrung und anschließende Reflektion kann auch zu einer allgemeinen Sensibilisierung für Sicherheitsthemen führen sowie zu Überlegungen, ob es im Unternehmen noch zu wenig beachtete Schwachstellen gibt, ob die vorhandenen Schutzmaßnahmen ausreichen, usw.

Ein solches Rollenspiel kann mit kleinen Teams durchgeführt werden, die die Aufgabe erhalten, ein bestimmtes Ziel zu erreichen (auf Rollenkarte vorgegeben, z. B. Zugriff auf geschützte Informationen erhalten, siehe unten bei „Mögliche Aufgaben für dieses Spiel“).

Aufgabenstellung: „Welches wäre das wirkungsvollste Vorgehen, um das vorgegebene Ziel zu erreichen?“

Bei diesem Beispiel handelt es sich nicht um ein vollständig realistisches Rollenspiel, sondern darum, sich möglichst intensiv in eine andere Rolle hineinzuversetzen und die entsprechenden Überlegungen anzustellen. Wesentlich ist dabei die Präsentation der Überlegungen vor weiteren Gruppenteilnehmern, entsprechendes Feedback und weitere Diskussion.

Hier können auch zwei (oder mehr) Teams an der gleichen Aufgabenstellung arbeiten und ihre Ergebnisse dann vergleichen. Falls ein „Wettbewerb“ positiv wirkt: Über den besten Ansatz abstimmen lassen.

Mögliche Aufgabenstellungen für dieses Spiel:

Als Innentäter z. B.

- Die Unterlagen von der letzten Vorstandsbesprechung einsehen,
- Die Gehaltshöhe des neuen Kollegen erfahren,
- Das System x zum Absturz bringen,
- Einem Kunden 100 Euro gutschreiben.

Als Außentäter z. B.

- Geld oder Wertgegenstände entwenden,
- Eine Abhöranlage / Kamera heimlich installieren,
- Eine vorhandene Kamera oder sonstige Überwachung außer Betrieb setzen,
- Einen wichtigen Zugangscode in Erfahrung bringen,
- Geheime Informationen (neues Produkt o. ä.) in Erfahrung bringen,
- Sabotage vorbereiten mit dem Ziel der Erpressung (Informationen, aber auch rein physisch),
- Eine Anlage oder ein Netzwerk zum Absturz bringen, Blackout bewirken.

Hierbei ist allerdings auch zu berücksichtigen, ob Situationen denkbar sind, wo jemand weiß, wie ein Angriff gelingen könnte, aber Sorge haben muss, dies offenzulegen, denn er würde sich damit „outen“ (hat Kenntnisse, die er/sie nicht haben dürfte, schwärzt damit Kollegen an, benennt Missstände an deren Beseitigung die meisten gar nicht interessiert sind bzw. die diese sogar verübeln würden, usw.). Es sollte die Möglichkeit bestehen, z. B. auch im Nachgang vertrauliche oder anonyme Beiträge zu liefern – siehe hierzu auch Kapitel 6.8.1.

6.5.3 Thema “Social Hacking” als Ausgangspunkt für weitere Rollenspiele

Im Folgenden wird das “Social Hacking” als Sonderfall des “Social Engineering” vorgestellt[17]. Auf dieser Grundlage können bei Bedarf passende Szenarien für Rollenspiele entworfen werden.

Beim Social Engineering werden Formen der sozialen Manipulation eingesetzt, um bestimmte juristisch und/oder moralisch fragwürdige Verhaltensweisen hervorzurufen, die die Betroffenen spontan und selbstbestimmt normalerweise nicht zeigen würden, und die einen direkten oder indirekten Schaden bei den Manipulierten selbst oder ihrem Unternehmen bewirken bzw. bewirken sollen. Wer Social Engineering einsetzt, nutzt also zwischenmenschliche Beziehungen, um unberechtigt Informationen zu erlangen oder Menschen zu schädlichen Handlungen zu verleiten. Dabei werden menschliche Eigenschaften wie Hilfsbereitschaft und Vertrauen genutzt, aber ebenso auch Angst und Respekt vor Autorität.

Wenn Social Engineering dem Eindringen in eine fremdes IT-System dient, um vertrauliche Daten einzusehen, das System zu korrumpieren oder sonstige Schäden zu bewirken, spricht man vom **Social Hacking.**

6.5.3.1 Arten des Social Hacking

Beim Social Hacking werden u. a. die folgenden Arten unterschieden:

- Phishing und Weiterentwicklungen:
  Versuche, über gefälschte Webseiten, E-Mails oder Kurznachrichten an persönliche Daten eines Internet-Benutzers zu gelangen und damit Identitätsdiebstahl zu begehen. Geschieht dies unter Nutzung bereits im Vorfeld beschaffter Informationen spricht man von „Spear-Phishing“.
  „Pharming“ basiert auf einer Manipulation der DNS-Anfragen von Webbrowsern, um den Benutzer auf gefälschte Websites umzuleiten. DNS-Anfragen können z.B. durch DNS-Spoofing, Cache Poisoning oder DNS-Hijacking verändert werden. Dazu kann vorher ein Trojanischen Pferd oder ein Virus passend platziert worden sein.
  Wenn sich der gezielte Phishing-Angriff gegen hohe Führungskräfte richtet, spricht man auch von „Whaling“.

- Dumpster Diving:
  Dumpster Diving meint das Durchsuchen des Mülls (oder des Papierkorb-Inhaltes) des Opfers nach Hinweisen über das soziale Umfeld und andere Informationen. Diese können dann in einem darauf folgenden gezielten Angriff genutzt werden, z.B.um das Vertrauen des Opfers zu erlangen.

- USB Drop:
  Auf verschenkten oder herumliegenden USB Sticks ist Schadcode enthalten, der auf

[17] Die Darstellung ist orientiert an einem Webinar von Prof. Dr. Harald Schaub, IABG, mit dem Titel „Social Hacking – Psychologische Grundlagen des Social Engineering oder Warum Firewalls nichts nützen“ (2019)

den Rechner geladen wird und sich von dort weiter verteilt, sobald der Stick am Rechner eingesteckt wird.

- Scareware:
  Bei dieser automatisierten Form des Social Hacking handelt es sich um ein Schadprogramm, das das Ziel hat, den Nutzen so zu ängstigen (scare), dass dieser bestimmte Handlungen durchführt, z. B. ein bestimmtes Programm lädt.

- Spam (oder Junk):
  Bezeichnung für meist unerwünschte, oft massenhaft und unverlangt gesendete Nachrichten (E-Mail, SMS, Telefon, Instant-Messaging-Dienst wie z. B. WhatsApp) mit werbendem Inhalt oder Lockangeboten. Oft wird verdeckt Schadsoftware mitgeschickt, die durch Download, Starten oder Aufrufen aktiviert werden kann.

- Persönlicher Kontakt:
  Eine Person wird dazu bewegt, aus einem positiven Gefühl heraus oder aus Unachtsamkeit einer anderen Person einen „Gefallen“ zu tun, der man das „Hacking“-Potenzial evtl. gar nicht ansieht. Es können aber auch Erpressung oder Bestechung zum Einsatz kommen.

6.5.3.2 Wirkungsweise des Social Hacking

Die Wirksamkeit des Social Hacking lässt sich vor allem durch die folgenden sozialpsychologischen Prinzipien erklären:

- Gehorsam und Konformität:
  Eine Person ändert ihr Verhalten aufgrund von Aufforderung durch eine Autoritätsperson oder durch den Konformitätsdruck der Situation[18]. Durch das Ausspielen von Hierarchieebenen und die Nutzung von Rollenerwartungen kann entsprechender Druck erzeugt werden.

- Foot-in-the-door Technique:
  Die Bereitschaft zum Ausüben einer Handlung wird erhöht, indem an die Person zunächst eine kleinere Bitte gerichtet wird, und die Person diese erfüllt. Bei der verwandten „Low-ball Technique“ hat eine zweite Anfrage die modifizierte Form einer ersten, harmloseren Anfrage.

- Reziprozitätsnorm:
  Der Empfänger einer Leistung fühlt sich zu einer Gegenleistung verpflichtet, auch wenn diese ggf. durch einen Fremden und ungefragt erfolgte.

[18] Siehe hierzu z. B. die themenbezogenen Untersuchungen „Milgram-Experimente“, „Zimbardo-Experimente“

- Soziale Bewährtheit:
  Personen orientieren sich bei Entscheidungen häufig am Handeln anderer Personen, die in der gleichen oder ähnlichen Situation sind. Bei Mehrdeutigkeit einer Situation wird die Aufmerksamkeit auf andere Personen gerichtet. Dies kann genutzt werden, um eine Person zu einer Handlung zu bewegen, indem ihr gesagt wird, dass andere Personen dies auch tun würden.

- Sympathiefalle / Liking-Bias:
  Personen lassen sich eher von Menschen beeinflussen, die sie sympathisch finden, z. B. wegen körperlicher Attraktivität, Ähnlichkeit mit der eigenen Person, Lob und Anerkennung, regelmäßigem Kontakt.

- Priming-Effekt
  Die Aufnahme eines ersten Reizes (Prime), beeinflusst die Interpretation nachfolgender Reize bzw. die Reaktion auf diese.

- Anker-Effekt:
  Menschen orientieren sich bei Entscheidungen an momentan verfügbaren Informationen in ihrer Umgebung (Anker). Dieser Anker bzw. die Information muss nicht zwingend relevant, sondern kann auch völlig willkürlich gewählt sein.

- Verzerrungsblindheit / Bias Blind Spot:
  Menschen sind gegenüber ihren eigenen Fehlern „blind“. Man teilt die Annahme, dass verzerrende Verhaltenseffekte zwar existieren, man selbst aber eine Ausnahme und nicht davon betroffen ist. Dies ist einer der stärksten verzerrenden Verhaltenseffekte.

6.5.3.3 Schutz vor Social Hacking

„Grundsätzlich ist jeder und jede im System empfänglich für Social Engineering.“[17]

Wichtig ist es, sich der möglichen Angriffspunkte bewusst zu sein und sich entsprechend zu verhalten. Hierbei helfen die folgenden Fragestellungen und Impulse weiter, anhand derer eine konkrete Situation beurteilt werden kann. Solche Fragestellungen können z. B. im Anschluss an ein Rollenspiel thematisiert werden.

- Kann ich der Person **vertrauen**, oder hat sie nur durch eine Taktik versucht, mein Vertrauen zu erlangen?
- Ist die Autoritätsperson tatsächlich ein Experte, oder wird **Autorität** nur durch Symbole vermittelt?
- Was sagt mein **Gefühl**? „Auch mal auf das eigene Bauchgefühl hören!“.
- Fühle ich mich zu etwas **verpflichtet**? (Siehe „Reziprozitätsnorm“ im vorausgehenden Kapitel 6.5.3.2). Hier sollte ggf. bewusst gegengesteuert werden.
- Wie würde die Situation **von außen betrachtet** auf einen Zuschauer wirken?

Man sollte sich eigentlich immer, aber gerade in solchen Situationen bewusst sein, dass man als Mensch ein sicherheitskritisches Element darstellt, das nicht vor kognitiven Denkfehlern oder Manipulationstechniken gefeit ist.

6.6 Coaching (on the job)

Als besondere Lehr- und Trainingsform sei hier auch das Coaching genannt. Es ist einerseits recht aufwendig, da ein besonders ausgebildeter Coach einen einzelnen Mitarbeiter betreut. Andererseits bietet keine andere Methode so gute Möglichkeiten, auf die individuelle Situation eines Mitarbeiters einzugehen und die Besonderheiten seiner Rollen und Aufgaben, sowie der Arbeitsumgebung und des institutionellen Umfeldes zu berücksichtigen. Die Ziele des Coachings werden individuell mit dem Mitarbeiter zusammen festgelegt, und schon hierbei sind im Hinblick auf die individuellen Voraussetzungen des Mitarbeiters wesentliche Weichenstellungen möglich, die den Lernerfolg begünstigen. Ein Coach gibt individuelle Anregungen und Feedback, steht für Fragen zur Verfügung und wahrt ggf. auch die angemessene Vertraulichkeit.

6.7 Enera-Lernplattform

6.7.1 Format des Angebotes

Das enera Qualifizierungscenter (eQC) ist eine orts- und zeitunabhängige Lernplattform, die allen enera-Projektbeteiligten zur Verfügung steht[19]. Neben reinen E-Learning-Kursen werden auch „klassische“ Seminare angeboten.

Zu Sicherheitsthemen werden seit 2018 zwei „eTrainings“ angeboten, die in den beiden folgenden Unterkapiteln kurz beschrieben werden:

- „Informationssicherheit“,
- „Informationssicherheit KRITIS“.

Die Buchungszahlen hierzu werden vom Lernplattform-Team als vergleichsweise gering bewertet, bis April 2020 gab es diese Zahlen:

- „Informationssicherheit“: 28 Buchungen.
  Alle wurden gestartet, 23 davon mit „bestanden“ abgeschlossen.
- „Informationssicherheit KRITIS“: 7 Buchungen.
  Alle wurden gestartet, 2 davon mit „bestanden“ abgeschlossen.

Die Einstellungen im Lernmanagementsystem (LMS) waren so gepflegt worden, dass ein Kurs erst als „bestanden“ gilt, sobald die lernende Person den Feedbackbogen ausgefüllt hat; dies sollte eine kleine Anreizwirkung darstellen. Die Erfahrung zeigte jedoch, dass die Trainings

[19] Siehe https://projekt-enera.de/blog/enera-podcast-sebastian-hartong-ueber-das-enera-qualifizierungscenter-eqc/.

gestartet und durchgearbeitet werden, am Ausfüllen der Feedbacks allerdings kaum mehr Interesse besteht[20]. Eine weitere Erläuterung hierzu: „Das Feedback kann von uns als enera Kompetenz- und Qualifizierungscenter (eQC) eingesehen werden & ist gänzlich anonymisiert. Der Standardeindruck von den Einheiten ist sehr gut; allerdings entsteht oftmals der Eindruck, dass die Fragen zum Abschluss nur zackig durchgeklickt werden, damit der Kurs als „bestanden“ angezeigt wird.“

Seit September 2020 wird ein weiteres e-Training zu Sicherheitsthemen auf der enera-Lernplattform angeboten, bei dem es um die „Sichere Lieferkette (SiLKe)“ für SMGW geht (siehe Kapitel 6.7.4), hierzu liegen jedoch noch keine Erfahrungen bzw. Rückmeldungen vor.

6.7.2 Beispiel eTraining „Informationssicherheit“

Das eTraining „Informationssicherheit“ ist an keine bestimmte Zielgruppe gerichtet. Es vermittelt Grundlagen zu den Themen Informationssicherheit, Maßnahmen für das sichere Verhalten und Social Engineering. Für jedes dieser drei Kapitel ist eine Bearbeitungszeit von jeweils ca. 30 Minuten vorgesehen.

Durch den Kurs führt nahezu durchgehend – unterbrochen durch ein Interview in Teil 1 und einen Telefon-Dialog in Teil 3 – die Journalistin, Autorin und Fernsehmoderatorin Petra Peschel als „Expertin für IT-Sicherheit“ auf sehr professionelle Art anhand verschiedener Beispiele und Erläuterungen, die jeweils im Bild dargestellt werden. Im zweiten Teil („Sicheres Verhalten“) wird u. a. auf der Suche nach Anhaltspunkten für ein Datenleck durch ein Mitarbeiter-Büro geführt (dort gibt es u. a. eine Haftnotiz mit Passwort und einen Papierkorb mit problematischem Inhalt), um so zu veranschaulichen, welche Verhaltensweisen am Arbeitsplatz von Sicherheitsrelevanz sind. Hier gibt es auch Hinweise zum richtigen Verhalten beim Arbeiten in der Öffentlichkeit.

Jedes der drei Kapitel schließt mit einem Selbst-Check ab. Ergänzt wird der Kurs durch einen ausführlichen Feedback-Fragebogen, der jedoch nicht genutzt wurde, siehe oben in Kapitel 6.7.

6.7.3 Beispiel eTraining „Informationssicherheit KRITIS“

Das eTraining „Informationssicherheit KRITIS“ umfasst die folgenden Themen:

- KRITIS und Bedrohungen
- Gesetze, Normen und Standards
- Maßnahmen entwickeln
- Prüfungen und Audits

Durch das Training führt ein nicht namentlich genannter Moderator, stellenweise ergänzt durch vorlesende Stimmen und den Auftritt weiterer Personen.

[20] Erschwerend könnte hier gewirkt haben, dass der Zusammenhang zwischen „Bestehen“ und Feedback-Funktion nicht für alle Nutzer auf Anhieb ersichtlich war.

Sehr authentisch wirkt der Bericht über Probleme bei einem „echten“ regionalen Energieversorger mit Auftritt des Geschäftsführers.

Dieses eTraining wurde nur von 7 Interessenten gestartet und nur in 2 Fällen abgeschlossen, siehe dazu auch oben in Kapitel 6.7.

6.7.4 Beispiel eTraining „Sichere Lieferkette (SiLKe)“

Das eTraining „Sichere Lieferkette (SiLKe)“ umfasst die folgenden Themen:

- Daten, Fakten und Hintergründe zum Einbau von SMGW und zu intelligenten Messsystemen mit kurzem Überblick zur gesetzlichen Grundlage und daraus resultierenden praktischen Konsequenzen für Messstellenbetreiber (MSB).
- Überblick über die Sichere Lieferkette (SiLKe) mit den Stationen Gateway-Hersteller (GWH), MSB und Einbauort.

Durch das Training führt eine nicht namentlich genannte Moderatorin, über weite Strecken vor einer aus Grafik-Elementen bestehenden Kulisse, die je nach Thema passende abstrakte oder schematische Darstellungen zeigt. Bei drei Gelegenheiten wird zur Interaktion durch Anklicken von markierten Stellen in der Bildschirmdarstellung aufgefordert, woraufhin ergänzende Erläuterungen angezeigt werden. Aufgelockert wird die Darstellung zu Beginn durch eine kurze „Störung“ der Energieversorgung mit unbekannter Ursache. Ein zwielichtig aussehender „Betrüger“ hat im weiteren Verlauf einige kurze wortlose – wie alle anderen Darstellungen eher symbolische - Auftritte, in denen er versucht, SMGW zu manipulieren oder zu stehlen. So ergibt sich als „roter Faden“, dass die Sichere Lieferkette vor Manipulation und schlimmstenfalls Blackout erfolgreich schützen kann. Eine Zielgruppe für das Training wird nicht explizit genannt; es handelt sich hier offenbar um einen ersten einführenden Überblick zum Thema.

Der abschließende Selbsttest umfasst 8 Fragen zu wesentlichen Kursinhalten und kann bei Bedarf beliebig oft bis zur vollständig richtigen Beantwortung wiederholt werden.

6.8 Weitere Möglichkeiten zur Sensibilisierung und Motivation für Sicherheitsthemen

Da einzelne Schulungen, Trainings und (Rollen-)Spiele nicht alleine eine nachhaltige Sensibilisierung für Sicherheitsthemen und dauerhaft regelkonformes Verhalten herbeiführen können, müssen sie durch weitere Maßnahmen ergänzt werden, die möglichst gut in eine unternehmensweite Sicherheitskultur (siehe Kapitel 4.4) integriert sind. Diese Maßnahmen sollen das Sicherheitsbewusstsein der Mitarbeiter stärken und ihre Bereitschaft zur Reaktion auf Sicherheitsvorfälle erhöhen. Hierzu gehört z. B. das Einrichten vertraulicher Meldewege (siehe Kapitel 6.8.1), die sichtbare Anerkennung von sicherheitsbewusstem Verhalten (siehe Kapitel 6.8.2) und eine möglichst motivierende allgemeine „Präsenz“ der Sicherheitsthemen (siehe Kapitel 6.8.3. ff.). Insgesamt ist eine Unternehmenskultur anzustreben, worin Sicherheitsbewusstsein und sicherheitsbewusstes Verhalten positiv besetzt sind und anerkannt werden, und wo entsprechend Versäumnisse und Verstöße nicht als Kavaliersdelikte toleriert werden.

Die in den folgenden Abschnitten dargestellten Umsetzungen und Beispiele stammen weitgehend aus Unternehmen beteiligter Konsortialpartner.

6.8.1 Vertrauliche Meldewege

Nicht immer ist es einem Mitarbeiter, der einen einmaligen oder fortgesetzten Sicherheitsvorfall miterlebt oder davon erfahren hat, leicht möglich zu beurteilen, ob hier für ihn selbst Handlungsbedarf besteht, was zu tun ist, wer zuständig ist bzw. an wen er sich wenden kann und soll. Hinzu kommt ggf. die Befürchtung persönlicher Nachteile durch direkte oder indirekte Konfrontation der Verursacher oder Beteiligten des Sicherheitsvorfalls oder durch Offenlegung eigener unberechtigter Kenntnisse, Zugänge o. ä.

Eine angemessene Reaktion auf Sicherheitsvorfälle oder unzulängliches sicherheitsbezogenes Verhalten kann u. a. durch die folgenden Maßnahmen und Möglichkeiten unterstützt werden:

- **Kommunikation der verantwortlichen Rollenträger und Ansprechstellen**
  Leicht zugängliche und stets aktuelle Informationen über die Aufgaben und Zuständigkeiten der Verantwortlichen für Informationssicherheit und Datenschutz im Unternehmen, ggf. auch weiterer Vertrauenspersonen, und ihre Erreichbarkeit.
- **Einrichtung anonymer Meldewege**
  Falls es zur Unternehmenskultur passt, kann die Einrichtung eines anonymen Briefkastens sinnvoll sein, mit restriktiven Regeln für den Zugang zu und dem Umgang mit dessen Inhalten auf Empfänger-Seite.
- **Transparenz**
  Ergänzend ist es wichtig, Transparenz über den Umgang mit Meldungen zu schaffen, ggf. auch in zusammengefasster Überblicks-Form, zum Schutz einzelner Betroffener. Ein Eindruck wie „es kümmert sich doch niemand darum“ wirkt demotivierend, und er sollte daher vermieden werden.

6.8.2 Newsletter und Events

Eine Möglichkeit, das Thema Informationssicherheit kontinuierlich präsent zu halten, die Sichtbarkeit der auf diesem Gebiet tätigen Instanzen zu verbessern und ggf. auch auf aktuelle Gefährdungen und erforderliche Maßnahmen hinzuweisen, ist ein **regelmäßiger Newsletter** an alle Mitarbeiter, der von der zuständigen Ansprechstelle herausgegeben wird.

Dies sind mögliche Rubriken in einem solchen Newsletter:

- Berichte über relevante Vorfälle mit Beispielen:
  - Dieser Angriff wurde abgewehrt – so gut sind wir schon!
  - Das ist passiert - vor so etwas wollen wir uns in Zukunft besser schützen!
- Berichte über im eigenen Unternehmen eingerichtete Vorkehrungen,
- Berichte von Mitarbeitern, die z. B. Phishing erkannt haben – Anerkennung für Wachsamkeit und sicherheitsbewusstes Verhalten,
- Berichte zu Aspekten des tatsächlich erreichten Sicherheitsniveaus, z. B.

    - So hoch ist die Versorgungssicherheit,
      ggf. auch im Vergleich zur Branche insgesamt – so gut sind wir schon!
- Weiterführende Informationen (Links, Hinweise zu Veranstaltungen usw.),
- „Das sind Ihre Ansprechpartner/Ansprechstellen“, ggf. mit Angabe der „Sprechstunde“,
- Beiträge von Mitarbeitern zu besonderen Vorkommnissen oder Fragen,
- „Bitte um Unterstützung bei …“,
- Interviews, Berichte aus dem Sicherheits-Alltag,
- Bericht „Eine Meldung und wie es danach weiterging“.

Bei Interesse könnte auch ein entsprechendes **Diskussionsforum** im Intranet eingerichtet werden, das den Teilnehmern ermöglicht, selbst am Thema beteiligt zu sein und nicht nur Sicherheitsvorgaben „von oben“ zu befolgen.

Bei einem **Sicherheitstag im Unternehmen** können Themen wie die oben genannten konzentriert und vertieft angeboten werden. Mögliche Formate sind z. B.:

- Kurzvorträge von Spezialisten (intern, extern),
- Talk-Runde mit der Unternehmensleitung oder anderen wichtigen Rollenträgern auf einer Bühne, durch die u. a. der Stellenwert der Informationssicherheit verdeutlicht werden kann,
- Informationsstände mit der Möglichkeit der Kontaktaufnahme und für Fragen.

Vorbereitend und ergänzend können Plakate und Merkblätter eingesetzt werden.

Ziel bei einem solchen Sicherheitstag ist es, die Mitarbeiter „abzuholen“ und ihr Interesse zu wecken. Dabei helfen ggf. auch unterhaltsame Beiträge im kabarettistischen Format.

Beispiel: Ein „Live Hacking“ zeigt Hacker und Mitarbeiter im teilweise sehr ironischen bis sarkastischen Dialog. Hierzu schreibt der Anbieter Allgeier CORE GmbH:

> „Wir sind der Meinung, dass IT- und Informationssicherheit auch mit einer Portion Spaß vermittelt werden kann. Bei dieser Herangehensweise treffen wir auf mehr Engagement und Interesse der Teilnehmer, die das Thema dadurch auch besser verinnerlichen. Deshalb präsentieren unsere Referenten eindrucksvolle Täter-Opfer-Rollenspiele, die aufzeigen, wie sich Mitarbeiter bei potenziellen Angriffen verhalten sollten.“[21]

6.8.3 Objekte, Bilder und Symbole

Objekte, Bilder und Symbole können das Themenfeld Informationssicherheit und angemessenes Verhalten in erfreulicher und angenehmer Weise im Alltag präsent halten. Sie können konzentriert viel aussagen, sie bleiben – wenn gut gemacht – lange im Gedächtnis, und sie informieren nicht nur, sondern lösen auch Gefühle aus. Ein Bezug zum Unternehmen ist leicht herzustellen durch entsprechendes Design und Layout.

[21] Zitat siehe: https://www.allgeier-core.com/news/presse/presse-details/allgeier-core-it-und-informationssicherheit-aus-einer-hand, Video siehe: https://www.allgeier-core.com/services/operations/security-awareness/live-hacking

Beispiel: In einem Unternehmen werden zunächst relevante Themen und jeweils zugehörige Verhaltensregeln und Hinweise identifiziert, wie sie z. B. auch auf Plakaten, Handzetteln und dgl. dargestellt werden. Pro Thema wird ein Kaffeebecher als „Sammeltasse“ in ansprechendem Design gestaltet, so dass diese Gefäße einen optisch erfreulichen Anblick bieten und man sie gerne auf dem Schreibtisch oder bei Besprechungen „vorzeigt“. Die Möglichkeit, mehrere unterschiedliche Exemplare besitzen zu können – möglichst in einem Kontext, wo sie als Anerkennung wirken, also z. B. als Gewinn in einem Sicherheits-Quiz – schafft einen Anreiz zum Sammeln und somit also auch, sich mit den Themen zu beschäftigen, und sei es zunächst oberflächlich. Die Präsenz der Tassen und der darauf sichtbaren Themen und Hinweise im Büroalltag sorgen im günstigen Fall dafür, dass diese Hinweise im Bewusstsein präsent sind und bleiben.

6.8.4 Inszenierung von Pseudo-Vorfällen

Die Inszenierung von Pseudo-Vorfällen ermöglicht es, die emotionale und i. d. R. erschreckende bzw. aufschreckende Wirkung eines realen Sicherheitsvorfalls auf die Betroffenen zu nutzen, um das Thema Informationssicherheit nachhaltig präsent zu machen, ohne jedoch die negativen Auswirkungen eines solchen Sicherheitsvorfalles in Kauf nehmen zu müssen. Ziel ist neben der konkreten Einzelfall-Thematik auch die allgemeine Sensibilisierung der Mitarbeiter für Sicherheitsrisiken.

Beispiel: In einem Unternehmen wird zunächst eine allgemeine Information zu Phishing Mails mit entsprechenden Warnungen an alle Mitarbeiter verschickt. Ca. 2 Wochen danach erhalten alle Mitarbeiter eine Mail, in der sie über ein neues bzw. aktualisiertes Teilsystem der internen IT informiert werden und aufgefordert werden, dieses System aufzurufen und sich dort mit Benutzername und Passwort anzumelden, um sich zu vergewissern, dass die Arbeit im System auch weiterhin wie gewohnt möglich ist. Dabei weichen Absenderangabe in der Mail und eine darin angegebene zu verwendende Web-Adresse in Details vom unternehmensüblichen Format ab, sie sind aber nicht auf Anhieb auffällig. Wer der Aufforderung folgt und sich unter dem in der Mail angegebenen Link anmeldet, sieht diesen Hinweis:

Ihre <Unternehmen/System>-Zugangsdaten
wurden gerade gestohlen!

Sie haben soeben Ihre <Unternehmen> -Zugangsdaten in eine nicht von <Unternehmen> betriebene Website eingegeben! Dieser Phishing-Test wurde von <Unternehmen> in Auftrag gegeben, um Sie für die Gefahren im Umgang mit dem Internet und E-Mail-Verkehr zu sensibilisieren.

Ergänzt wird diese Mitteilung durch den Verweis auf ein für alle Mitarbeiter zugängliches Online-Training zum Thema, die Ankündigung einer Information zu den Ergebnissen des Phishing-Tests (sie sollte neutral gehalten sein, um im Falle sehr negativer Ergebnisse diese ggf. nicht in Image-schädigender Weise offenlegen zu müssen) und die Bitte, Kollegen nicht zu warnen, um die Ergebnisse des Tests nicht zu verfälschen.

Kurze Zeit danach erhalten alle Mitarbeiter eine Mail, in der von der Durchführung des Phishing-Test berichtet wird, und in der die Warnungen wiederholt werden. Ergänzend wird auf Anleitungen zur Änderung des Passworts hingewiesen für solche Fälle, in denen der Mitarbeiter befürchtet bzw. befürchten sollte, dass das Passwort nicht mehr sicher ist.

Im Anschluss an eine solche Inszenierung kann eine Befragung der Mitarbeiter sinnvoll sein, warum sie auf eine solche Mail „hereingefallen" sind. Mitarbeiter-Beiträge in Form von freiwilligen Angaben nach entsprechender Einladung, z. B. in der Sprechstunde des Sicherheitsbeauftragten (oder auch über vertrauliche Meldewege, siehe Kapitel 6.8.1) können Verbesserungsmöglichkeiten aufzeigen, z. B. um zukünftig die Gefahr zu verringern, dass auf echte Phishing-Mails, deren Absender eine vermeintlich existierende Geschäftseinheit des Unternehmens ist, falsch reagiert wird.

6.8.5 "Lessons Learned" / Debriefing

Die (idealerweise) beim Abschluss externer und interner Projekte oder vergleichbarer Arbeiten durchgeführte abschließende Auswertung der jeweils gemachten Erfahrungen in Form einer "Lessons Learned"-Veranstaltung bietet eine gute Gelegenheit, auch auf Themen der Informationssicherheit einzugehen – nicht nur hinsichtlich realer Vorfälle und erfolgreicher Vorkehrungen usw., sondern auch im Hinblick auf Voraussetzungen, Aufwände und Ergebnisse bei der Identifikation, Berücksichtigung und Umsetzung relevanter Sicherheitsanforderungen. Hieraus ergeben sich i. d. R. hilfreiche Erkenntnisse zu den folgenden Aspekten:

- Voraussetzungen und Randbedingungen der Arbeiten, wie z. B. Verfügbarkeit relevanter Standards und Normen, Erreichbarkeit von Ansprechpartnern, Regelungen im Informationssicherheitskonzept / ISMS,
- Umgang mit bekannten Gefährdungen und Risiken,
- Neu erkannte Gefährdungen und Risiken,
- Erfahrungen zu Unternehmens-interner und -externer Zusammenarbeit, Partnerschaften, Informationsschnittstellen usw.

Wenn eine solche Auswertung von mehreren unterschiedlichen Projektbeteiligten – wie z. B. Auftraggeber und Auftragnehmer – gemeinsam durchgeführt wird, kann es hilfreich sein eine Software zu nutzen, die Beiträge anonymisiert „einsammelt". Dies senkt erfahrungsgemäß die Hemmschwelle, ggf. auch kritische oder „heikle" Themen anzusprechen.

Wichtig ist auch für einen solchen Erfahrungsaustausch eine Gesprächs- und Unternehmenskultur, in der Sicherheitsbewusstsein positiv besetzt ist und entsprechend anerkannt wird.

7 Scope-übergreifend relevante Erkenntnisse, Ergebnisse und Festlegungen

7.1 Attraktivität von Kursen zur Informationssicherheit

Die auf der enera-Lernplattform angebotenen Kurse zur Informationssicherheit stießen nach aktuellen Erkenntnissen im Projekt enera nur auf geringes Interesse. Von den ohnehin geringen Nutzerzahlen (siehe Kapitel 6.7.1) sind noch solche Nutzer abzuziehen, die seitens AP12 einen Eindruck von den Kursen gewinnen wollten. Vor diesem Hintergrund ergab sich die Überlegung, dass Gamification (siehe Kapitel 5.1.3) hier einen positiven Effekt haben würde, also zu mehr Interesse an Themen der Informationssicherheit führt. Deshalb wurde beim Konsortialpartner OFFIS ein Point-and-Click-Adventure in Auftrag gegeben (siehe Kapitel 6.2.2) dessen Entwicklung aktuell noch nicht abgeschlossen ist. Interessensbekundungen im Vorfeld („Wann können wir denn mal testen?“) lassen jedoch bereits jetzt eine positive Resonanz erwarten.

7.2 Interesse an Sicherheitsthemen in anderen enera-Arbeitspaketen

Das relativ geringe beobachtete Interesse anderer enera-Arbeitspakte an Schulungsinhalten und sonstigen Möglichkeiten zur Information über oder zum Austausch zum Thema Informationssicherheit ist erklärlich im Licht einiger Thesen, die seitens AP12 auch schon für die enera-Abschlussdokumentation formuliert wurden. Informationssicherheit war in keinem der anderen Arbeitspakte ein wesentliches Thema u. a. aus den folgenden Gründen:

- Die Konsortialpartner hatten vielfach Sicherheitsthemen bereits vorab geregelt und umgesetzt, unabhängig vom Projekt.
- Einzelpersonen, die sich bei einer Projekt-Aufgabe mit Sicherheitsaspekten befassten, waren mit der Materie bereits vertraut.
- Die Projektergebnisse entstanden vielfach ohne konkrete Zukunftsperspektive über den Projektabschluss hinaus, und es gab entsprechend kein relevantes Schadenspotenzial durch Sicherheitsprobleme.

Es hatte also in anderen AP entsprechend keine hohe Priorität, sich mit solchen Themen zu befassen, und die vorhandenen Angebote wirkten offenbar nicht hinreichend verlockend für eine Beschäftigung damit aus „reinem“ Interesse.

8 Zusammenfassung und Ausblick

Die Themen, die im AS 12.2.17 „Schulung und Sensibilisierung zur Informationssicherheit“ betrachtet wurden, ergaben sich weniger aus unmittelbar anstehenden Projektaufgaben bei

enera, sondern weitgehend aus einem generellen Interesse im AP12 beteiligter Konsortialpartner, vorhandene Möglichkeiten für die Schulung und Sensibilisierung zu Sicherheitsthemen zu beschreiben und zu bewerten, um in dieser Hinsicht Anregungen für eigene Aktivitäten zu erhalten. Hierbei stand besonders die Zielgruppe „Management“ im Fokus, da sie einerseits einen großen Einfluss auf die Sicherheitskultur im Unternehmen hat, und andererseits ein attraktives Ziel für personenbezogene Angriffe darstellt.

Die Analyse der Zielgruppe Management und der für diese Zielgruppe relevanten Inhalte und Methoden ergibt, dass Schulung und Sensibilisierung möglichst flexibel und individuell zu gestalten sind, dass aber vielfach auf solche Formate zurückgegriffen werden kann, die auch für andere Zielgruppen eingesetzt werden. Bei den relevanten Inhalten für die Zielgruppe Management handelt es sich einerseits um allgemeine Themen, die für alle Mitarbeiter relevant sind, und andererseits um solche, die vor allem durch das Management gestaltet und geprägt werden: Die Unternehmenskultur, die Sicherheitskultur im Unternehmen und das davon stark beeinflusste Sicherheitsbewusstsein aller Unternehmensangehörigen liegen im Verantwortungsbereich des Managements, das dementsprechend informiert und sensibilisiert sein muss.

Damit aus der „Schwachstelle Mensch“ ein „Sicherheitsfaktor Mensch“ im Unternehmen wird, reicht es nicht aus, einmalig oder punktuell zu schulen und zu sensibilisieren, sondern bei allen Mitarbeitern muss das Sicherheitsbewusstsein permanent wachgehalten und gefördert werden. Entsprechend wurden in AS 12.2.17 einzelne Formate und Beispiele für Schulung und Sensibilisierung aus der Erfahrungswelt der Konsortialpartner beschrieben und bewertet.

Dabei erwies sich, dass die sog. Gamification, also die Übertragung von spieltypischen Elementen und Vorgängen in spielfremde Zusammenhänge wie z. B. ein Sicherheitstraining, offenbar sehr motivierend sein kann, sich mit Sicherheitsthemen zu befassen; dass dies auch für das Management gilt, zeigt u. a. das Beispiel „Escape Game/Escape Room“ (siehe Kapitel 6.1.2). Interesse und Feedback zu den Gamification-Beispielen waren weit intensiver und positiver als zu den „konventionellen“ Angeboten auf der enera-Lernplattform. Es handelt sich bei der Gamification also um einen tragfähigen Ansatz, der auf jeden Fall für Einstieg und Motivation zum Thema geeignet ist. Einige spezielle Sicherheitsthemen und eine vertiefte Schulung zu bestimmten Sicherheitstechnologien können damit aber voraussichtlich nicht angemessen abdeckt werden.

Es zeigte sich auch, dass die bloße Existenz der jeweiligen Angebote zu Schulung und Sensibilisierung alleine nicht ausreicht – die Angebote müssen auch im Unternehmen gut sichtbar sein, und um eine nachhaltige Wirkung zu entfalten, müssen sie in eine entsprechende Sicherheitskultur im Unternehmen eingebettet sein.

Um die richtige Balance zwischen Interesse, Motivation und Spass auf der einen Seite und der Vermittlung von fachlichen Inhalten zu erreichen und aufrecht zu erhalten kann es zukünftig sinnvoll sein, solche Formate, die bei der Einführung bzw. beim erstmaligen Einsatz erfolgreich sind (z.B. bestimmte Games), kontinuierlich weiter zu entwickeln und gleichzeitig nach und nach fachlich tiefergehende Themen anzusprechen und/oder aktuelle Entwicklungen zu berücksichtigen, bis Kenntnisse und Bewusstsein i. S. von „Gewahr-Sein (awareness)“ bei der Zielgruppe auf dem erforderlichen Niveau aktiv nutzbar vorhanden sind. Die Mitarbeiter sollen somit eine Methodik erleben, die ihnen grundsätzlich schon vertraut ist (d.h. sie sollen nicht

überfordert werden), die aber immer wieder auch neue Aspekte und Überraschungen enthält (d.h. es soll keine Langeweile entstehen). Im Idealfall kann in diesem Prozess die Anhebung des inhaltlichen/fachlichen Niveaus parallel erfolgen.

Die Bereitstellung von zielgruppengerechten und inhaltlich aktuellen Methoden und Inhalten für die Schulung und Sensibilisierung zu Sicherheitsthemen wird somit auch in Zukunft eine permanente Aufgabe sein, für die es keine einmalige „ideale“ Lösung gibt. Dies bedingen nicht zuletzt der allgemeine technische Fortschritt, entsprechend neuartige Spezialisierungen von Aufgaben und Kompetenzen und das erforderliche Schritthalten mit immer neuen Bedrohungslagen. Vor diesem Hintergrund müssen auch Schulung und Sensibilisierung immer wieder neu und möglichst individuell auf die Anforderungen und Bedürfnisse der Zielgruppen eingehen. Dabei können zukünftig neue bzw. bisher noch selten für solche Zwecke eingesetzte Technologien unterstützen, z. B. aus dem Bereich der künstlichen Intelligenz und des Machine Learning, und es können Trainings in virtuellen Umgebungen angeboten werden, die durch vollständige 3D-Virtualisierung „lebensechte“ und entsprechend eindrucksvolle Erfahrungen ermöglichen.

9 Anlagen

- **Anlage 1: Konzept Escape Room** – Schulungswerkzeug zur Informationssicherheit
  Autor: EWE Netz
  Stand: 01.02.2019
  Dateiname: AS12.2.17_Anlage 1_20190201_Darstellung_Escape_Game.pptx

- **Anlage 2**: **Schulungskonzept Zielgruppen** – Übersicht der Zuordnung von Inhalte und Medien zu unterschiedlichen Zielgruppen entsprechend der relevanten Zielgruppen-Charakteristika.
  Autor: EWE Netz
  Stand: 02.10.2019
  Dateiname: AS12.2.17_Anlage 2_20191002_Schulungskonzept Zielgruppen.xlsx

10 Bezugsdokumente

Nr.	Bezeichnung	Inhalt	Link / Ablageort / Datei
1	**Ergebnisdokument AS 12.2.1**	„Gesetze, Regularien, Richtlinien, Compliance, Zertifizierungen“	enera Sharepoint: 2017-09-20_AS12.2.1_Gesetze, Regularien, Richtlinien, Compliance, Zertifizierungen_V1.03.docx
2	**Ergebnisdokument AS 12.2.2 und AS 12.2.6**	„Festlegung grundsätzliche Vorgehensweise (IT + OT Security)“ und „Überschneidungen analysieren und allgemeingültige Schritte zur Etablierung von ISMS“	enera Sharepoint: 20180410_AS12.2.2u6_Festlegung Vorgehensweise_allg Schritte_Ueberschn_ ISMS_V1.00.docx
3	**Ergebnisdokument AS 12.2.3**	„ISMS Werkzeuge“	enera Sharepoint: 20180124_Ergebnisdokument AS 12.2.3_v1.1.docx
4	**Ergebnisdokument AS 12.2.4**	„Governance, Compliance und Datenschutz: Erhebungen, Strukturen und Management“ *Folgedokument zu AS 12.2.1*	enera Sharepoint: 2018-12-07_AS12.2.4_Governance, Compliance und Datenschutz_V1.11.docx
5	**Ergebnisdokument AS 12.2.5**	„Strukturierung der Systemlandschaft und IV/ Scopes festlegen	enera Sharepoint: 20180417_Ergebnisdokument_12.2.5_Strukturierung-Scopes_V1.02.docx
6	**Ergebnisdokument AS 12.2.7**	„Strukturanalyse und Inventarisierung“	enera Sharepoint: 20181221_Ergebnisdokument AS12.2.7_Strukturanalyse_Inventarisierung_V1.00.docx
7	**Ergebnisdokument AS 12.2.8**	„Schutzbedarfsfeststellung“	enera Sharepoint: 20190205_AS12.2.8_Schutzbedarfsfeststellung_V1.00.docx
8	**Ergebnisdokument AS 12.2.10**	„Risikobehandlung“ (Meilensteinbericht Stand 05.04.2019)	enera Sharepoint: 20190405_AS12.2.10_Risikobehandlung_V0.02.docx
9	**ISO/IEC 27000-Reihe**	ISO 27000 („Rahmen“) ISO 27001 (ISMS) ISO 27002 (Maßnahmen) ISO/IEC 27019 (Erweiterung der Norm ISO/IEC 27002 auf den Bereich der Prozessleit- und Automatisierungstechnik in der Energieversorgung.)	https://www.iso.org/
10	**BSI IT-Grundschutz**	**BSI-Standard 200-1**: Managementsysteme für Informationssicherheit (ISMS), Version 1.0, Stand 2017-10 **BSI-Standard 200-2**:	https://www.bsi.bund.de/

Nr.	Bezeichnung	Inhalt	Link / Ablageort / Datei
		IT-Grundschutz-Methodik, Version 1.0, Stand 2017-10. **BSI-Standard 200-3**: Risikoanalyse auf der Basis von IT-Grundschutz, Version 1.0, Stand 2017-10. **IT-Grundschutz-Kompendium** 2. Edition 2019 3. Edition 2020	
11	**IT-Sicherheitskatalog**	IT-Sicherheitskatalog gemäß §11 Absatz 1a Energiewirtschaftsgesetz der Bundesnetzagentur (BNetzA) - für Betreiber von Strom- und Gasnetzen (August 2015) - für Betreiber von Energieanlagen (Dezember 2018)	https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Energie/Unternehmen_Institutionen/Versorgungssicherheit/IT_Sicherheit/IT_Sicherheitskatalog_08-2015.pdf *sowie* <…>/ IT_Sicherheitskatalog_2018.pdf
12	**TR-03109**	BSI TR-03109 Technische Vorgaben für intelligente Messsysteme und deren sicherer Betrieb mit **BSI TR-03109** Dachdokument **BSI TR-03109-1** Anforderungen an die Interoperabilität der Kommunikationseinheit eines intelligenten Messsystems **BSI TR-03109-2** Anforderungen an die Funktionalität und Interoperabilität des Sicherheitsmoduls **BSI TR-03109-3** Kryptographische Vorgaben für die Infrastruktur von intelligenten Messsystemen **BSI TR-03109-4** Smart Metering PKI **BSI TR-03109-6** Smart Meter Gateway Administration	https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03109/index_htm.html
13	**ITGS-Baustein INF.5 (CD)**	INF.5 Raum oder Schrank für technische Infrastruktur (Stand: November 2018) Seitens BSI gab es hierzu im Juni 2019 die Aussage, dass dieser Baustein demnächst als überarbeiteter CD erneut veröffentlicht und in die Edition 2020 des ITGS-Kompendiums aufgenommen werden soll. Ende Juli 2019 wurde der Baustein nach Abschluss der Kommentierungsphase unverändert wieder veröffentlicht.	https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-Grundschutz-Modernisierung/BS_Schutzschrank.html sowie: enera Sharepoint / AP12 /AS 12.2.09-(…) / BS_Schutzschrank__INF_5.pdf

Nr.	Bezeichnung	Inhalt	Link / Ablageort / Datei
14	**Schutzprofil Smart Meter Gateway**	Schutzprofil Smart Meter Gateway (**BSI-CC-PP-0073**)	https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/SmartMeter/SmartMeterGateway/Schutzprofil_Gateway/schutzprofil_smartmetergateway_node.html
15	**Entwurf zum IT-Sicherheitsgesetz 2.0**	Referentenentwurf des Bundesministeriums des Innern, für Bau und Heimat - **Entwurf eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme** (IT-Sicherheitsgesetz 2.0 – IT-SiG 2.0)	http://intrapol.org/wp-content/uploads/2019/04/IT-Sicherheitsgesetz-2.0-_-IT-SiG-2.0.pdf

Tabelle 2: Bezugsdokumente

11 Abbildungsverzeichnis

Abbildung 1: Abhängigkeit der Arbeitsschritte in TAP 12.2 zur Einführung des enera-ISMS .. 8

12 Tabellenverzeichnis

Tabelle 1: Einzelne Aspekte von Schulungsveranstaltungen: Vor- und Nachteile 28
Tabelle 2: Bezugsdokumente 56

Ergebnisdokument AS 12.2.19

„Incident Handling (IH)“

Autoren:

Konrad Rosmus, Ulrike Henschel (IABG mbH)

03.07.2019

Gefördert durch:

aufgrund eines Beschlusses
des Deutschen Bundestages

Historie des Dokuments

Version	Datum	Name	Änderungen	Dateiname
0.01	02.07.2019	Ulrike Henschel, IABG	Erstfassung	20190702_AS12.2.19_Incident Handling_V0.01.docx
0.02	03.07.2019	Ulrike Henschel, IABG	Kommentare und Korrekturen von Konrad Rosmus sind eingearbeitet	20190703_AS12.2.19_Incident Handling_V0.02.docx
1.0	----	----	Version, Dateiname. Freigegebene Version 1.0 = Version 0.02	2019-07-03_AS12.2.19_Incident Handling_V1.0.docx

Inhalt

Abkürzungsverzeichnis 4
1 Einleitung 5
2 Verantwortlichkeiten und Pflichten 6
3 Verhaltensregeln und Meldeweg bei Auftreten eines Sicherheitsvorfalls 7
3.1 Meldeweg 8
3.2 Eskalationsstrategie bei Sicherheitsvorfällen 8
3.2.1 Kategorien von Sicherheitsvorfällen 9
3.2.2 Schwere von Sicherheitsvorfällen 9
3.2.3 Eskalation 10
3.3 Prioritätensetzung 11
3.4 Methodik zur Untersuchung und Bewertung von Sicherheitsvorfällen 11
3.5 Umsetzung von Maßnahmen zur Behebung von Sicherheitsvorfällen 13
3.6 Benachrichtigung betroffener Stellen 16
3.7 Nachbereitung eines Sicherheitsvorfalls 17
4 Einsatz von Detektionsmaßnahmen für Sicherheitsvorfälle 17
5 Effizienzprüfung und Aktualisierung 18
6 Veröffentlichung der Festlegungen zur Behandlung von Sicherheitsvorfällen 18
7 Bezugsdokumente 19
8 Abbildungsverzeichnis 19
9 Tabellenverzeichnis 19

Abkürzungsverzeichnis

Abkürzung	Bedeutung
Admin	Administration
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSIG	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz)
HW	Hardware
IDS	Intrusion Detection System
IH	Incident Handling
IPS	Intrusion Prevention System
IS	Informationssicherheit
ISB	Informationssicherheitsbeauftragter
IT	Informationstechnik
KRITIS	Kritische Infrastrukturen
SW	Software

Ergebnisdokument AS 12.2.19

„Incident Handling (IH)“

1 Einleitung

Die Behandlung von Sicherheitsvorfällen – das Security Incident Handling – ist Teil des Informationssicherheitsmanagements[1] der Energieversorger, Netz- und Messstellenbetreiber sowie weiterer Dienstleister bzw. Marktteilnehmer im Bereich Smart Grid und Smart Market. Dies ist in einer entsprechenden Richtlinie angemessen zu regeln. Dabei sind ggf. auch die Vorgaben für die Betreiber von „Kritischen Infrastrukturen“[2] (KRITIS) zu beachten.

Es ist festzulegen, dass und wie Sicherheitsvorfälle und Sicherheitsprobleme gemeldet werden. Die Entscheidungsfindungs- und Verarbeitungswege sind zu beschreiben, Verantwortlichkeiten und Pflichten sind festzulegen.

Sicherheitsvorfällen müssen systematisch untersucht und bewertet werden. Die Reaktionen bei den Sicherheitsvorfällen müssen sinnvoll und angemessen sein. Dazu ist eine vorausgehende Vorbereitung und Planung notwendig.

Da bei der Behandlung von Sicherheitsvorfällen unterschiedliche organisatorische und technische Aspekte berücksichtigt werden müssen, ist die Einbindung mehrerer Personen bzw. Rollen und Interessensgruppen erforderlich.

Neben der Leistungsfähigkeit der Unternehmen im Bereich Smart Grid und Smart Market zur Erfüllung ihrer Kernaufgaben spielen die Belange des Datenschutzes, das Arbeits- und Strafrecht, Haftungsfragen etc. eine Rolle.

Nachfolgend ist ein Rahmen für die Behandlung von Sicherheitsvorfällen dargestellt. Die spezifischen Einzelaspekte sind vom IS-Management-Team des jeweiligen Unternehmens zusammen mit den entsprechenden Personen und Gremien festzulegen und in einer entsprechenden Richtlinie an alle Mitarbeiter zu kommunizieren.

Weitere Hinweise und Beispiele finden sich u. a. in den thematisch zugeordneten Bausteinen „Detektion und Reaktion“ (DER) des IT-Grundschutz-Kompendiums des BSI [1].

Ein besonderer Bereich der Behandlung von Sicherheitsvorfällen ist das Notfallmanagement (enera AS 12.2.21 Notfallmanagement / Continuity Management), das hier nicht weiter betrachtet wird. Die Entscheidung darüber, ob ein Notfall vorliegt oder nicht, wird jedoch innerhalb des Incident Handling getroffen.

---

[1] Informationssicherheit umfasst als Oberbegriff auch IT-Sicherheit und Datensicherheit.

[2] Organisationen oder Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden. Hierzu gehört u. a. der Sektor „Energie“.

2 Verantwortlichkeiten und Pflichten

Beim Auftreten von Sicherheitsvorfällen bestehen für die einzelnen **Rollen** folgende Pflichten:

Leitung des Unternehmens

- Abschließende Entscheidungsfindung
- bei Bedarf Vorbereitung der Informationspolitik bezüglich des Sicherheitsvorfalls
- Einschaltung des Eskalationswegs über die eigene Organisation des Unternehmens hinaus
- Veranlassung notwendiger Maßnahmen
- Veranlassung der Überprüfung des Informationssicherheitsmanagements
- Bewertung der Ergebnisse der Nachbereitung eines Sicherheitsvorfalls

Bereichs-/Abteilungsleitungsebene des Unternehmens

- bei Bedarf Vorbereitung der Informationspolitik bezüglich des Sicherheitsvorfalls
- Entgegennahme von Meldungen zu Sicherheitsproblemen und -vorfällen und Abwägung der Bewertung zwischen Sicherheitsvorfällen und Störfallen ohne Sicherheitsbezug
- Einschaltung des Eskalationswegs
- Einleitung und Abwicklung notwendiger Maßnahmen
- Überprüfung des Informationssicherheitsmanagements
- Nachbereitung eines Sicherheitsvorfalls
- Etablieren von Schulungen der Mitarbeiter des IT-Betriebs zur Annahme und Behandlung von Sicherheitsvorfällen

Informationssicherheitsbeauftragter (ISB)

- Einschaltung des Eskalationswegs
- Einleitung und Abwicklung notwendiger Maßnahmen
- Überprüfung des Informationssicherheitsmanagements
- Nachbereitung eines Sicherheitsvorfalls

Informationssicherheitsmanagement-Team (IS-Management-Team)

- Einschaltung des Eskalationswegs
- Einleitung und Abwicklung notwendiger Maßnahmen
- Überprüfung des Informationssicherheitsmanagements
- Nachbereitung eines Sicherheitsvorfalls
- Im Falle eines schwelenden Sicherheitsproblems: Vorschlag einer Lösungsstrategie

IT-Systemadministration

- Entgegennahme von Meldungen und erste Entscheidungsvorbereitung zwischen Sicherheitsproblem bzw. -vorfall und Störfall sowie Einleitung der Eskalation
- Durchführung/Umsetzung der technischen Maßnahmen zur Schadensfeststellung, Schadensbegrenzung, Wiederherstellung und Beweissicherung
- Teilnahme an Schulungen zur Annahme und Behandlung von Sicherheitsvorfällen

Mitarbeiter in Haustechnik, Verwaltung und Kundendienst

- Meldung von Sicherheitsproblemen und -vorfällen

Fremdpersonal, Fernwartungspersonal

- Meldung von Sicherheitsproblemen und -vorfällen

Die Verantwortlichkeiten sind zu regeln und in Kraft zu setzen.

Bei einem schwierigen oder schwerwiegenden Sicherheitsvorfall bilden der Informationssicherheitsbeauftragte, der Leiter des Unternehmens und der Leiter der IT bzw. IT-Systemadministration zeitlich befristet das **Sicherheitsvorfall-Team**. Dessen Befugnisse beinhalten:

- Durchführung von HW- und SW-Konfigurationen zur Behebung der Folgen eines Sicherheitsvorfalls
- Einleitung von Maßnahmen zur Identifikation der Ursachen eines Sicherheitsvorfalls
- Information der Mitarbeiter über sie betreffende Folgen eines Sicherheitsvorfalls und ggf. resultierende Einschränkungen
- Entscheidung über die Notwendigkeit der Eskalation an andere Stellen

Die Leitung des Sicherheitsvorfall-Teams liegt beim Leiter des Unternehmens.

3 Verhaltensregeln und Meldeweg bei Auftreten eines Sicherheitsvorfalls

Für die effektive Behandlung von Sicherheitsvorfällen ist entscheidend, dass sich Betroffene richtig und besonnen verhalten und den Vorfall unverzüglich weitermelden. Dazu sind die Verhaltensregeln (Ruhe bewahren, Meldepflicht, Auskunftspflicht über Begleitumstände, etc.) zu fixieren und die Betroffenen sind entsprechend zu informieren.

3.1 Meldeweg

Jeder Sicherheitsvorfall ist zunächst der IT-Systemadministration zu melden. Die IT-Systemadministration erhält somit die Aufgabe, Meldungen über sicherheitsrelevante Unregelmäßigkeiten, die mit den betreuten IT-Systemen, -Anwendungen und Netzen verbunden sind, entgegenzunehmen. Anschließend ist entsprechend festgelegter Definitionen und Schwellwerte[3] zu entscheiden, ob es sich um eine einfache Störung ohne Sicherheitsbezug[4] oder um einen Sicherheitsvorfall handelt.

Entsprechend der Bewertung wird eine einfache Störung ohne Sicherheitsbezug durch die IT-Systemadministration selbst behoben. Über einen Sicherheitsvorfall sind der Informationssicherheitsbeauftragte (ISB) und die Leitungsebene zu unterrichten.

Der ISB nimmt Meldungen über Sicherheitsvorfälle entgegen. Er führt die Untersuchung und Bewertung des Vorfalls durch. Er wählt notwendige Maßnahmen aus und veranlasst deren Umsetzung, soweit dies nicht seinen Kompetenzbereich überschreitet. Bei Bedarf ruft er das Sicherheitsvorfall-Team zusammen bzw. unterrichtet zur Eskalation die Leitungsebene. Bei schweren Sicherheitsvorfällen sowie Notfällen[5] ist der Notfallbeauftragte einzubeziehen

3.2 Eskalationsstrategie bei Sicherheitsvorfällen

Je kritischer ein Sicherheitsvorfall ist, desto mehr Kompetenzen werden bei der Behandlung des Sicherheitsvorfalls in der Regel benötigt. Dies kann so weit führen, dass die Leitung des Unternehmens informiert und eingeschaltet werden muss, um notwendige Maßnahmen wie Verbot der Informationsweitergabe, Einschaltung der Polizei, kostenträchtige Ersatzmaßnahmen etc. einleiten zu dürfen. Sicherheitsvorfälle können unterschiedlichster Art sein (Kapitel 3.2.1) und unterschiedlich schwerwiegend (Kapitel 3.2.2) sein. Für diese Einstufungen sind eine Reihe von Einflussfaktoren (potentielle Schadenshöhe und Folgeschäden, Ursache, betroffene IT-Systeme/ -Anwendungen und Netze, notwendige Sofortmaßnahmen) zu erheben und zu bewerten.

Nach Eingang einer Meldung über eine sicherheitsrelevante Unregelmäßigkeit wird unter diesen Voraussetzungen entschieden, ob es sich um ein lokales Sicherheitsproblem oder um einen Sicherheitsvorfall mit ggf. zu erwartenden größeren Schäden handelt. Bei Bedarf sind gemäß einer Eskalationsstrategie die nächsten Managementebenen und der Notfallbeauftragte einzubeziehen.

[3] Diese Abgrenzungen müssen in Abhängigkeit vom Schutzbedarf der betroffenen Geschäftsprozesse, IT-Dienste, IT-Systeme bzw. IT-Anwendungen verbindlich festgelegt und kommuniziert werden.
[4] Ein Störfall ohne Sicherheitsbezug kann z. B. Stromausfall oder das Versagen einer Festplatte sein.
[5] Hierunter wird i. d. R. ein länger andauernder Ausfall von Prozessen oder Ressourcen mit hohem oder sehr hohem Schaden verstanden, dessen Behandlung eine besondere Notfallorganisation erfordert.

3.2.1 Kategorien von Sicherheitsvorfällen

Für Unternehmen in den Bereichen Smart Grid und Smart Market werden folgende Kategorien von Sicherheitsvorfällen definiert:

Sicherheitsvorfälle verursacht durch eigenes/beauftragtes Personal/Innentäter

- Unautorisierte Zutrittsversuche
- Unautorisierte Zugangs- und Zugriffsversuche
- Daten- bzw. SW-Manipulation durch Innentäter
- Sicherheitsvorfälle bei der Fernwartung

Sicherheitsvorfälle verursacht durch Außentäter

- Unautorisierte Zutrittsversuche durch Außenstehende
- Hacking-Versuche (erfolglos) durch Außentäter
- Eindringen in das Netzwerk bzw. die Systeme („erfolgreicher Hacking-Versuch“)

Sicherheitsvorfälle verursacht durch Innen- oder Außentäter, Folgeschäden

- Auftreten eines Computer-Virus, SW-Anomalien
- HW-Zerstörung/Manipulation
- Fehlverhalten des Systems, Dienstausfall

3.2.2 Schwere von Sicherheitsvorfällen

Zur Beurteilung der Schwere bzw. Tragweite von Sicherheitsvorfällen werden folgende Einstufungen festgelegt:

Unkritisch

Es sind nur wenige Systeme betroffen bzw. Systeme, die keine kritischen Funktionen betreffen. Es sind nur wenige Daten mit normalem Schutzbedarf betroffen. Weitere Infrastrukturen (z. B. vor- und nachgelagerte Netzbetreiber, Wasserversorgung) sind nicht betroffen.

Mittel

Es sind einige Systeme betroffen bzw. Systeme, die eher unkritische Funktionen betreffen. Es sind im Wesentlichen Daten mit normalem Schutzbedarf betroffen. Es besteht die Möglichkeit, dass personenbezogene oder firmenvertrauliche Daten betroffen sind. Weitere Infrastrukturen (z. B. vor- und nachgelagerte Netzbetreiber, Wasserversorgung) sind nur in geringem Ausmaß betroffen.

Hoch

Die Funktionsfähigkeit des gesamten Unternehmens, insbesondere die Erfüllung der Kernaufgaben, ist gefährdet. Es sind viele wichtige Systeme und Datenbestände betroffen. Weite-

re Infrastrukturen (z. B. vor- und nachgelagerte Netzbetreiber, Wasserversorgung) werden an der Erfüllung ihrer Kernaufgaben so stark gehindert, dass sie sie nicht mehr erfüllen können. In besonders schweren Fällen, in denen durch Auswirkungen auf die Verfügbarkeit z. B. Gefahren für Leib und Leben eintreten können, muss die Entscheidung getroffen werden, ob es sich um einen Notfall handelt und die entsprechenden Maßnahmen sind ggf. einzuleiten.

3.2.3 Eskalation

Kategorie und Schwere eines Sicherheitsvorfalls bestimmen die Eskalation (d.h. wer zu benachrichtigen ist) gemäß folgender Eskalationsstrategie:

Legende:

Admin:	Ergreifen von Maßnahmen durch die IT-Systemadministration nach eigenem Ermessen.
ISB:	Information des Informationssicherheitsbeauftragten
Leitung:	Information der Leitung des Unternehmens bzw. Stellvertreter

Gegebenenfalls ist bei Sicherheitsvorfällen mit Schweregrad „hoch“ auch der Notfallbeauftragte einzubeziehen.

Schwere des Sicherheitsvorfalls ► ▼ Kategorie Sicherheitsvorfall	Unkritisch	Mittel	Hoch
Unautorisierte Zutrittsversuche durch Innentäter	Admin	Leitung	Leitung
Unautorisierte Zugangs- und Zugriffsversuche d. Innentäter	Admin	ISB	ISB
Daten- bzw. SW-Manipulation durch Innentäter	Admin	ISB	Leitung
Sicherheitsvorfälle bei der Fernwartung	ISB	ISB	Leitung
Unautorisierte Zutrittsversuche durch Außenstehende	ISB	Leitung	Leitung
Hacking-Versuche (erfolglos) durch Außentäter	Admin	Admin	ISB
Eindringen in das Netzwerk bzw. die Systeme	ISB	ISB	Leitung

Schwere des Sicherheitsvorfalls ► ▼ Kategorie Sicherheitsvorfall	Unkritisch	Mittel	Hoch
Auftreten eines Computervirus, SW-Anomalien	Admin	Admin	ISB
Fehlverhalten des Systems, Dienst-ausfall	Admin	Leitung	Leitung
HW-Zerstörung/Manipulation	Admin	ISB	Leitung

Tabelle 1: Eskalation von Sicherheitsvorfällen - Eskalationsstrategie

3.3 Prioritätensetzung

Da ein Sicherheitsvorfall meist aus einer Verkettung verschiedener Ursachen entsteht und auch Auswirkungen auf verschiedene betroffene IT-Anwendungsbereiche besitzt, sollten die zu treffenden Maßnahmen anhand einer Prioritätenliste umgesetzt werden. Diese Prioritätensetzung hängt vom Schutzbedarf und von den IT-Einsatzbereichen und -Anwendungen ab. Für die Unternehmen im Bereich Smart Grid und Smart Market sollen die aus einem Sicherheitsvorfall resultierenden Schäden in einer sachgerechten, effizienten und wirtschaftlichen Reihenfolge bearbeitet werden. Dies ist im Einzelfall durch das IS-Management-Team festzulegen. Folgende Prioritätensetzung kann als Anhaltspunkt dienen:

1) Verhinderung von Schäden an Leib und Leben
2) Wiederherstellung des Betriebs und der Versorgungssicherheit
3) Begrenzung der finanziellen Auswirkungen
4) Verhinderung von Manipulationen an HW, SW und Daten
5) Verhinderung der Offenlegung von internen Informationen
6) Vermeidung von Ansehensverlust

3.4 Methodik zur Untersuchung und Bewertung von Sicherheitsvorfällen

Um bei einem Sicherheitsvorfall die angemessenen Maßnahmen ergreifen zu können, ist dieser nach dem Melden/Erkennen zunächst zu bewerten. Als Entscheidungsgrundlage dafür sind die wesentlichen Einflussgrößen zu bestimmen. Diese variieren nach Art des Vorfalls. Für die Organisation eines Unternehmens im Bereich Smart Grid und Smart Market kann die folgende Zuordnung gelten. Die Einflussgrößen werden im Anschluss an die Tabelle erläutert.

Zu erhebende Einflussgröße ► ▼ Kategorie Sicherheitsvorfall	A	B	C	D	E	F	G	H	I	J	K	…	…
Unautorisierte Zutrittsversuche durch Innentäter	x				x	x							
Unautorisierte Zugangs- und Zugriffsversuche d. Innentäter	x	x	x		x	x							
Daten- bzw. SW-Manipulation durch Innentäter	x			x	x	x	x	x	x				
Sicherheitsvorfälle bei der Fernwartung[6]	x	x	x		x	x	x	x			x		
Unautorisierte Zutrittsversuche durch Außenstehende	x				x	x							
Hacking-Versuche (erfolglos) durch Außentäter	x					x					x		
Eindringen in das Netzwerk bzw. die Systeme	x	x	x	x	x	x	x	x	x	x	x		
Auftreten eines Computervirus, SW-Anomalien	x	x	x	x	x	x	x	x	x	x	x		
Fehlverhalten des Systems, Dienstausfall	x			x	x	x	x	x	x				
HW-Zerstörung/Manipulation	x	x	x	x	x	x	x	x	x				

Tabelle 2: Einflussgrößen bei der Bewertung von Sicherheitsvorfällen

Die relevanten Einflussgrößen sind:

(A) Welche IT-Systeme, -Anwendungen und Netze können von dem Sicherheitsvorfall zusätzlich betroffen sein?

(B) Können Folgeschäden, auch durch die Vernetzung der IT-Systeme, entstehen?

(C) Für welche IT-Systeme, -Anwendungen und Netze können Schäden und Folgeschäden ausgeschlossen werden?

(D) Wie hoch kann der durch den Sicherheitsvorfall verursachte direkte Schaden oder Folgeschaden sein?

[6] Fernwartung durch externen Dienstleister

(E) Wodurch wurde der Sicherheitsvorfall ausgelöst, z. B. durch Unachtsamkeit, Angreifer (bekannt?) oder Ausfall der Infrastruktur?

(F) Wann und an welcher Stelle hat sich der Sicherheitsvorfall ereignet?

(G) Ist die Kommunikationsinfrastruktur betroffen?

(H) Wie weit sind die Kommunikationsmöglichkeiten eingeschränkt?

(I) Geht vom jetzigen Zustand des Unternehmens eine Gefahr für andere Unternehmen oder Dritte aus?

(J) Wie viele Informationen über den Sicherheitsvorfall sind bereits an die Öffentlichkeit gedrungen?

(K) Ist bei anderen Unternehmen (vergleichbaren oder Vertretungs-Dienstleistern oder Marktteilnehmern) der gleiche Vorfall aufgetreten?

(…) *Ggf. weitere Einflussgrößen nach unternehmensspezifischen Erfordernissen.*

Die Erhebung der Einflussfaktoren erfolgt im Wesentlichen durch die IT-Systemadministration, ggf. unterstützt durch den Informationssicherheitsbeauftragten (ISB).

3.5 Umsetzung von Maßnahmen zur Behebung von Sicherheitsvorfällen

Bei der Umsetzung der notwendigen Maßnahmen zur Behebung von Sicherheitsvorfällen und ggf. zur Wiederherstellung der Betriebsumgebung ist unter Abwägung von zeitlichen Bedingungen mit der angemessenen Sorgfalt vorzugehen. Die Umsetzung der Maßnahmen ist ausreichend zu dokumentieren. Darüber hinaus sollte – vorsätzliches Handeln bei Sicherheitsvorfällen vorausgesetzt – auch die Behandlung des "Täters" mitbedacht werden. Die durchzuführenden Maßnahmen richten sich nach Art und Schwere des Vorfalls. Die folgende Auflistung skizziert eine mögliche sinnvolle Vorgehensweise:

Kategorie Sicherheitsvorfall	Maßnahmen zur Behebung
Unautorisierte Zutrittsversuche durch Innentäter	**Sofortmaßnahmen** - Täter feststellen und befragen - Feststellung der vom Eindringling durchgeführten Aktionen - Beseitigung offensichtlicher Schwachstellen bei der Zutrittssicherung falls möglich
	Mittel-/langfristige Maßnahmen - Review und Verbesserung von Zutrittssicherungsstrategie/-konzept

Kategorie Sicherheitsvorfall	Maßnahmen zur Behebung
Unautorisierte Zugangs- und Zugriffsversuche d. Innentäter	**Sofortmaßnahmen** - Täter feststellen und befragen - Feststellung der vom Eindringling durchgeführten Aktionen - Sperren des Accounts
	Mittel-/langfristige Maßnahmen - Review und Verbesserung von Zugangs-/Zugriffsschutzstrategie/-konzept
Daten- bzw. SW-Manipulation durch Innentäter	**Sofortmaßnahmen** - Täter feststellen und befragen - Sperren des Accounts - Restauration der Daten/SW soweit möglich
	Mittel-/langfristige Maßnahmen - Review und Verbesserung Zugriffsschutzstrategie/-konzept - Forensische Untersuchung des Schadens
Sicherheitsvorfälle bei der Fernwartung	**Sofortmaßnahmen** - Fernwartungszugang abschalten - Analyse des Schadens - Restauration der Konfiguration bzw. Daten/SW soweit möglich - Kontaktaufnahme zur Fernwartungsfirma - Verständigung anderer Dienstleister oder Marktteilnehmer
	Mittel-/langfristige Maßnahmen - Verbesserung der Sicherheitsfunktionen zur Fernwartung - Anpassung der vertraglichen Regelung
Unautorisierte Zutrittsversuche durch Außenstehende	**Sofortmaßnahmen** - Täter feststellen und befragen - Feststellung der vom Eindringling durchgeführten Aktionen - Beseitigung offensichtlicher Schwachstellen bei der Zutrittssicherung falls möglich

Kategorie Sicherheitsvorfall	Maßnahmen zur Behebung
	Mittel-/langfristige Maßnahmen - Review und Verbesserung von Zutrittssicherungsstrategie/-konzept
Hacking-Versuche (erfolglos) durch Außentäterl	**Sofortmaßnahmen** - Protokollierung
	Mittel-/langfristige Maßnahmen - Auswertung der Protokollierung
Eindringen in das Netzwerk bzw. die Systeme	**Sofortmaßnahmen** - Herunterfahren von Systemen - Trennung der Vernetzung - Spurensicherung für späterer forensische Untersuchung - Warnung anderer Dienstleister oder Marktteilnehmer
	Mittel-/langfristige Maßnahmen - Forensische Untersuchung des Schadens bzw. der Ursachen - Verbesserung der Absicherung der LAN
Auftreten eines Computervirus, SW-Anomalien	**Sofortmaßnahmen** - Verhinderung der Ausbreitung - Warnung anderer Dienstleister oder Marktteilnehmer - Beseitigung
	Mittel-/langfristige Maßnahmen - Überprüfung der Virenschutzstrategie - Forensische Untersuchung des Schadens bzw. der Ursachen
Fehlverhalten des Systems, Dienstausfall	**Sofortmaßnahmen** - Aktivierung Ausweichmöglichkeiten - ggf. Informierung anderer Dienstleister oder Marktteilnehmer
	Mittel-/langfristige Maßnahmen - Forensische Untersuchung des Schadens

Kategorie Sicherheitsvorfall	Maßnahmen zur Behebung
	bzw. der Ursachen
HW-Zerstörung/Manipulation	**Sofortmaßnahmen** - Aktivierung Ausweichmöglichkeiten
	Mittel-/langfristige Maßnahmen - Reparatur oder Ersatzbeschaffung - Feststellung des Täters

Tabelle 3: Maßnahmen zur Behebung von Sicherheitsvorfällen

Für die Initiierung und Überwachung der aufgeführten Maßnahmen ist der Informationssicherheitsbeauftragte (ISB) zuständig. Die Umsetzung erfolgt im Wesentlichen durch die IT-Systemadministration, in Einzelfällen durch den ISB. Die Vorgänge werden vom Bearbeiter dokumentiert.

3.6 Benachrichtigung betroffener Stellen

Alle betroffenen internen Stellen sind zeitnah zu informieren, ggf. unter Einbeziehung von Datenschutzbeauftragtem, Mitarbeitervertretung und Juristen. Sollte sich herausstellen, dass ein Sicherheitsvorfall in den Auswirkungen nicht nur auf das Unternehmen beschränkt ist, muss zur Schadensminimierung eine Benachrichtigung der evtl. betroffenen Stellen erfolgen.

Für erhebliche IT-Störungen im Betrieb der „Kritischen Infrastrukturen“[2] (KRITIS) sieht § 8b BSIG [2] unter anderem eine Meldepflicht für die KRITIS-Betreiber an das BSI vor, damit organisationsübergreifende IT-Störungen durch Warnungen oder Absicherungshinweise des BSI an andere KRITIS-Betreiber verhindert oder abgemildert werden können. Nähere Hinweise dazu, was unter einer erheblichen IT-Störung zu verstehen ist, sowie zum Meldeweg finden sich auf der entsprechenden Homepage[7] des BSI.

[7] https://www.bsi.bund.de/DE/Themen/Industrie_KRITIS/KRITIS/IT-SiG/Neuregelungen_KRITIS/Meldepflicht/meldepflicht_node.html

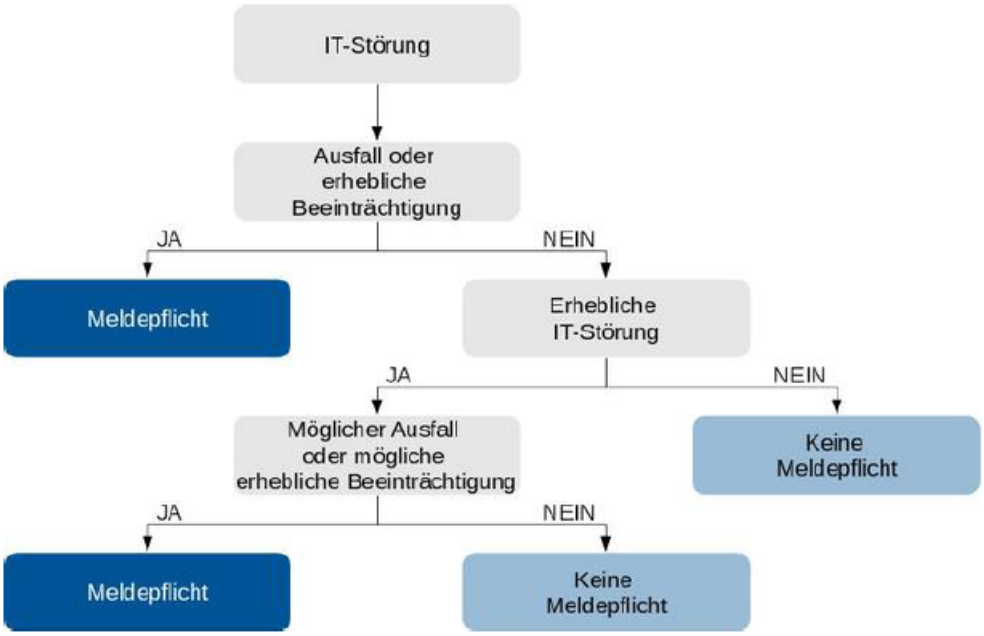


Abbildung 1: KRITIS: Meldekriterien für IT-Störungen (Quelle: BSI)

3.7 Nachbereitung eines Sicherheitsvorfalls

Um den Lerneffekt eines eingetretenen Sicherheitsvorfalls nicht zu vernachlässigen, sollte für die Behandlung von Sicherheitsvorfällen die Nachbereitung festgelegt werden. Oftmals lassen sich daraus Verbesserungen für den Umgang mit Sicherheitsvorfällen herausarbeiten oder Rückschlüsse auf die Wirksamkeit der Informationssicherheitskonzeption ziehen. Dabei sind unter anderem folgende Aspekte zu beachten:

- Reaktionszeit,
- Bekanntheitsgrad des Meldewegs,
- Wirksamkeit der Eskalationsstrategie,
- Effektivität der Untersuchung und
- Möglichkeiten der Benachrichtigung betroffener Stellen.

Für die Nachbearbeitung von Sicherheitsvorfällen ist das IS-Management-Team zuständig.

4 Einsatz von Detektionsmaßnahmen für Sicherheitsvorfälle

Je schneller ein Sicherheitsvorfall entdeckt und gemeldet wird, umso effektiver können Gegenmaßnahmen ergriffen werden. Hierbei kann es sinnvoll sein, die technisch möglichen Detektionsmaßnahmen zu nutzen, um Verzögerungen durch menschliches Handeln zu reduzieren. Grundsätzlich kommen hierfür u. a. in Frage:

- Viren-Suchprogramme,
- Auswertungen von Protokolldaten (unter Einhaltung der geltenden gesetzlichen Regelungen zum Datenschutz)
- Intrusion-Detection-/Intrusion-Prevention-Systeme (IDS/IPS)

Über die konkrete Notwendigkeit zum Einsatz weiterer Werkzeuge zur Erkennung von Schadcode oder Anomalien (unter Berücksichtigung des Aufwandes) entscheidet das IS-Management-Team.

Die regelmäßige Sensibilisierung und Schulung der Mitarbeiter ist eine weitere Maßnahme, die zur frühzeitigen Entdeckung sicherheitsrelevanter Vorfälle beitragen kann.

Weitere Hinweise und Beispiele finden sich u. a. in dem thematisch zugeordneten Baustein „Detektion von sicherheitsrelevanten Ereignissen“ (DER.1) des aktuellen IT-Grundschutz-Kompendiums des BSI [1].

5 Effizienzprüfung und Aktualisierung

Um die Effektivität eines Managementsystems zur Behandlung von Sicherheitsvorfällen messen zu können und um die notwendige Praxis dieser Managementaufgaben zu fördern, sind ggf. Übungen bzw. Planspiele durchzuführen.

Über konkrete Aktionen dazu (unter Berücksichtigung des Aufwandes) entscheidet das IS-Management-Team.

Die Wirksamkeit des Managementsystems zur Behandlung von Sicherheitsvorfällen wird anlassbezogen im IS-Management-Team diskutiert. Die entsprechende Richtlinie wird bei Bedarf überprüft und ergänzt. Eine Überprüfung erfolgt zudem mindestens jährlich.

6 Veröffentlichung der Festlegungen zur Behandlung von Sicherheitsvorfällen

Die Festlegungen zur Behandlung von Sicherheitsvorfällen, insbesondere auch Zuständigkeiten und Meldewege, sollten den Mitarbeitern wie folgt bekannt gegeben werden:

- Veröffentlichung der Richtlinie im Intranet
- Aufnahme in die jeweiligen Arbeitsplatzbeschreibungen
- Hinweise im jährlichen Personalgespräch
- Übergabe eines entsprechenden Merkblattes bei der Einstellung

7 Bezugsdokumente

Nr.	Bezeichnung	Inhalt	Link / Ablageort / Datei
1	**BSI IT-Grundschutz**	**BSI-Standard 200-1**: Managementsysteme für Informationssicherheit (ISMS), Version 1.0, Stand 2017-10 **BSI-Standard 200-2**: IT-Grundschutz-Methodik, Version 1.0, Stand 2017-10. **BSI-Standard 200-3**: Risikoanalyse auf der Basis von IT-Grundschutz, Version 1.0, Stand 2017-10. **IT-Grundschutz-Kompendium** 2. Edition 2019	https://www.bsi.bund.de/
2	**BSI-Gesetz**	**Gesetz über das Bundesamt für Sicherheit in der Informationstechnik**	https://www.bsi.bund.de/DE/DasBSI/Gesetz/gesetz_node.html

Tabelle 4: Bezugsdokumente

8 Abbildungsverzeichnis

Abbildung 1: KRITIS: Meldekriterien für IT-Störungen (Quelle: BSI) 17

9 Tabellenverzeichnis

Tabelle 1: Eskalation von Sicherheitsvorfällen - Eskalationsstrategie 11
Tabelle 2: Einflussgrößen bei der Bewertung von Sicherheitsvorfällen 12
Tabelle 3: Maßnahmen zur Behebung von Sicherheitsvorfällen 16
Tabelle 4: Bezugsdokumente 19

Ergebnisdokument AS 12.2.21

„Notfallmanagement / Continuity Management“

Anlage: Rahmendokument für eine Leitlinie zum Notfallmanagement

Autoren:

Konrad Rosmus, Ulrike Henschel (IABG mbH), Christine Rosinger (OFFIS)

16.01.2020

Gefördert durch:

Bundesministerium
für Wirtschaft
und Energie

aufgrund eines Beschlusses
des Deutschen Bundestages

Historie des Dokuments

Version	Datum	Name	Änderungen	Dateiname
0.01	02.10.2019	Ulrike Henschel, IABG	Erstfassung	2019-10-02_AS12.2.21_Anlage 1 Rahmen Leitlinie_V0.01.docx
0.02	25.10.2019	Christine Rosinger, OFFIS	Kommentierung und Ergänzung	2019-10-25_AS12.2.21_Anlage 1 Rahmen Leitlinie_V0.02.docx
0.03	06.12.2019	Ulrike Henschel, IABG	Fortschreibung	2019-12-06_AS12.2.21_Anlage 1 Rahmen Leitlinie_V0.03.docx
0.04	16.01.2020	Ulrike Henschel, IABG	Aufnahme weiterer Änderungen nach Abstimmung mit OFFIS	2020-01-16_AS12.2.21_Anlage 1 Rahmen Leitlinie_V0.04.docx
1.0	11.12.2020	Christine Rosinger, OFFIS	Dokument zu einer 1.0 gemacht, damit finalisiert.	2020-12-11_AS12.2.21_Rahmen Leitlinie Notfallmanagement_V1.0.docx

Inhalt

Abkürzungsverzeichnis 4
1 Einleitung 5
1.1 Einordnung 5
1.2 Gliederung 6
2 Vorgehen bei der Erstellung der Leitlinie zum Notfallmanagement 7
3 Inhalte einer Leitlinie zum Notfallmanagement 9
3.1 Definition des Notfallmanagements 9
3.1.1 „Notfall“ – Definition und Abgrenzung 10
3.2 Geltungsbereich des Notfallmanagements 10
3.3 Stellenwert des Notfallmanagements für das Unternehmen 10
3.4 Zielsetzung und Kernaussagen der Notfallstrategie 11
3.5 Vorgehensmodell für das Notfallmanagement 12
3.6 Verantwortlichkeiten und Pflichten 12
3.7 Aufrechterhaltung und Weiterentwicklung des Notfallmanagements 13
3.8 Zu beachtende Gesetze, Richtlinien und Vorschriften 14
3.9 Übernahme der Verantwortung durch die Unternehmensleitung 14
4 Bezugsdokumente 15
5 Abbildungsverzeichnis 16
6 Tabellenverzeichnis 16

Abkürzungsverzeichnis

Abkürzung	Bedeutung
AP	Arbeitspaket
AS	Arbeitsschritt
BCM	Business Continuity Management
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSIG	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz)
IH	Incident Handling
IS	Informationssicherheit
ISMS	Informationssicherheitsmanagementsystem
ISB	Informationssicherheitsbeauftragter
IT	Informationstechnik
KRITIS	Kritische Infrastrukturen
SINTEG	Schaufenster intelligente Energie - Digitale Agenda für die Energie-wende
TAP	Teilarbeitspaket

Ergebnisdokument AS 12.2.19

Anlage 1: „Rahmendokument für eine Leitlinie zum Notfallmanagement“

1 Einleitung

Dieses (Rahmen-)Dokument wurde während des Projekts enera entwickelt. **Enera** ist eins der fünf durch das Bundesministeriums für Wirtschaft und Energie (BMWi) geförderten Projekte des Förderprogramms „Schaufenster intelligente Energie – Digitale Agenda für die Energiewende“ (SINTEG)[1]. Im Projekt werden Lösungen zu den drei Themenschwerpunkten Netz, Markt und Daten in der Modellregion im Nordwesten Niedersachsens entwickelt und erprobt. Das **Arbeitspaket (AP) 12** innerhalb dieses Projekts beschäftigt sich mit der informationstechnischen Entwicklung der enera Gesamtarchitektur inklusive eines Informationssicherheitskonzepts.

Das **Teilarbeitspaket (TAP) 12.2** befasst sich mit dem Informationssicherheitskonzept; der zugehörige **Arbeitsschritt (AS) 12.2.21** behandelt das Notfallmanagement und das Continuity Management (Kontinuitätsmanagement, auch Business Continuity Management (BCM)). Das hier entstandene Rahmendokument für eine Leitlinie zum Notfallmanagement wird als Anlage dem Ergebnisdokument für AS 12.2.21 beigefügt. Es soll Verantwortliche in der Domäne der Energiewirtschaft dabei unterstützen, in ihrem Unternehmen eine Leitlinie für das Notfallmanagement zu erstellen.

1.1 Einordnung

Ziel des Informationssicherheitsmanagements[2] der Energieversorger, Netz- und Messstellenbetreiber sowie weiterer Dienstleister bzw. Marktteilnehmer im Bereich Smart Grid und Smart Market ist die kontinuierliche und vollständige Informationssicherheit, wobei ggf. auch die Vorgaben für die Betreiber von „Kritischen Infrastrukturen“[3] (KRITIS) zu beachten sind. Das Notfallmanagement ist dabei ein Bestandteil des Informationssicherheitsmanagements. Die **Aufrechterhaltung** der Informationssicherheit ist **im Hinblick auf besonders schwere Sicherheitsvorfälle**, die als Notfälle qualifiziert werden, in ein übergreifendes Notfallmanagement einzubinden, worin die in einem Notfall erforderlichen Prozesse geplant, etabliert und

[1] Siehe auch die Seite des SINTEG-Förderprogramms auf der Homepage des BMWi https://www.bmwi.de/Redaktion/DE/Artikel/Energie/sinteg.html.
[2] Informationssicherheit umfasst als Oberbegriff auch IT-Sicherheit und Datensicherheit.
[3] Organisationen oder Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden. Hierzu gehört u. a. der Sektor „Energie“.

überprüft werden. Die Gefährdungslage umfasst z. B. den Ausfall von Personal, IT-Systemen, Netzverbindungen, Gebäuden und Infrastruktureinrichtungen, Lieferanten oder Dienstleistern.

Im Notfallmanagement sind daher geeignete Maßnahmen zu identifizieren und umzusetzen, durch die einerseits alle relevanten Prozesse und Assets robuster und ausfallsicherer gemacht werden, und durch die andererseits bereits eingetretenen Notfälle schnell und zielgerichtet bewältigt werden können.

Die Maßnahmen des Notfallmanagements sind wiederum in ein ganzheitliches Kontinuitätsmanagement einzubetten. Siehe hierzu und zum Notfallmanagement allgemein z. B.

- IT-Grundschutz-Kompendium [1], Baustein DER.4 Notfallmanagement
- BSI-Standard 100-4 zum Notfallmanagement [4]
- Zukünftiger BSI-Standard 200-4 (Fortschreibung des Standard 100-4) zum „Business Continuity Management – BCM“ (voraussichtliche Bezeichnung), der sich z. Zt. in der Weiterentwicklung befindet.[4]

Nachfolgend ist ein Rahmen für eine Leitlinie zum Notfallmanagement dargestellt, in der alle wesentlichen Aspekte des Notfallmanagements thematisiert werden. Die spezifischen Einzelaspekte sind innerhalb eines solchen Rahmens vom Notfallmanagement-Team des jeweiligen Unternehmens zusammen mit den entsprechenden Personen und Gremien festzulegen. Die Leitlinie zum Notfallmanagement ist an alle Mitarbeiter zu kommunizieren.

Auf Basis dieser Leitlinie kann u. a. das Notfallhandbuch für das jeweilige Unternehmen erstellt werden. Es enthält detaillierte Informationen zu Rollen, Sofortmaßnahmen, Alarmierung und Eskalation sowie zu Plänen hinsichtlich Kommunikation, Geschäftsfortführung, Wiederanlauf und Wiederherstellung während und nach Notfallsituationen.

Weitere Hinweise und Beispiele finden sich u. a. in den thematisch zugeordneten Bausteinen „Detektion und Reaktion“ (DER) des IT-Grundschutz-Kompendiums des BSI [1].

Die Entscheidung darüber, ob ein Notfall vorliegt oder nicht, wird nicht innerhalb des Notfallmanagements selbst, sondern beim Incident Handling (IH) getroffen. Siehe hierzu auch AS 12.2.19 Incident Handling [7].

1.2 Gliederung

Dieses Dokument als Rahmendokument einer Leitlinie für Notfallmanagement gliedert sich im weiteren Verlauf wie folgt:

- Kapitel 2 enthält Hinweise zum Vorgehen bei der Erstellung einer Leitlinie für Notfallmanagement.
- Kapitel 3 enthält zu allen wesentlichen Inhalten einer solchen Leitlinie jeweils ein Unterkapitel mit Beschreibung und Hinweisen zu Zielen und Umsetzung.

[4] Zum aktuellen Stand der Arbeiten am BSI-Standard 200-4 siehe z. B. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BCM/BCM_20190416_Infomail.html

2 Vorgehen bei der Erstellung der Leitlinie zum Notfallmanagement

„Bevor ein Notfallmanagement institutionsweit etabliert werden kann, sind zunächst die Rahmenbedingungen zur Umsetzung des Notfallmanagements festzulegen. Diese Rahmenbedingungen und Ziele des Notfallmanagements werden in einer sogenannten Leitlinie dokumentiert. Zentrale Inhalte sind der Geltungsbereich des Notfallmanagements, Kernaussagen zur Notfallstrategie und die Übernahme der Verantwortung durch die Leitung der Institution. Die Leitlinie zum Notfallmanagement ist das zentrale Strategiedokument im Notfallmanagement.“ (Zitat aus: Umsetzungsrahmenwerk Notfallmanagement [5], Kapitel 3).

Für die Erstellung und Herausgabe einer Leitlinie zum Notfallmanagement durch ein Unternehmen gelten Vorgaben und Hinweise im BSI-Standard 100-4 [4]. Ergänzend zum Standard gab das BSI ein umfangreiches Umsetzungsrahmenwerk [5] heraus, das zu einzelnen sog. Modulen – wie z. B. der Leitlinie – spezifische Hilfsmittel anbietet. Dazu gehört eine Dokumentvorlage für einen Leitfaden mit Ausfüllanleitung sowie eine beispielhafte Präsentations-Vorlage, die bei der Erstellung der Leitlinie genutzt werden kann, um eine gemeinsames Verständnis von Aufgaben und Zielen herzustellen. Die beiden Abbildungen in diesem Kapitel sind dieser Präsentation entnommen.

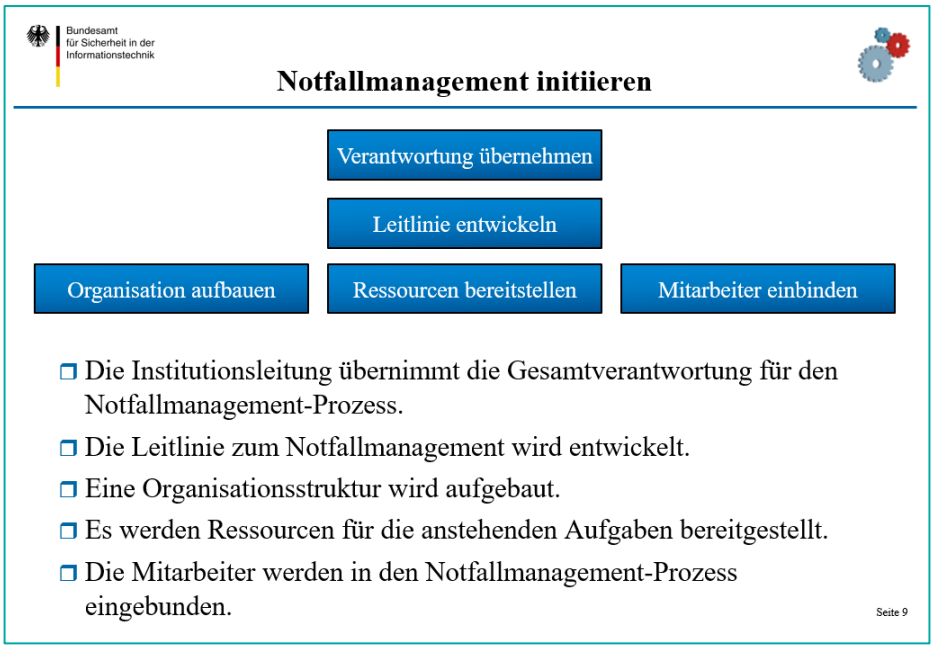


Abbildung 1: Notfallmanagement initiieren (Quelle: BSI [5])

Der Stellenwert der Leitlinie zum Notfallmanagement ergibt sich u. a. daraus, dass sie bereits sehr früh bei der Einführung des Notfallmanagements in einem Unternehmen erarbeitet und kommuniziert wird. In ihr sind die wesentlichen Ziele und Regelungen enthalten, die die Grundlage für sämtliche weiteren Arbeiten und Festlegungen zum Notfallmanagement bilden. Hierin ist sie z. B. vergleichbar mit einer Leitlinie zur Informationssicherheit und deren Funktion für

die Ausgestaltung eines ISMS, wie sie für enera im Arbeitsschritt AS 12.2.16 erarbeitet wurde (siehe das zugehörige Ergebnisdokument AS 12.2.16 [6]).

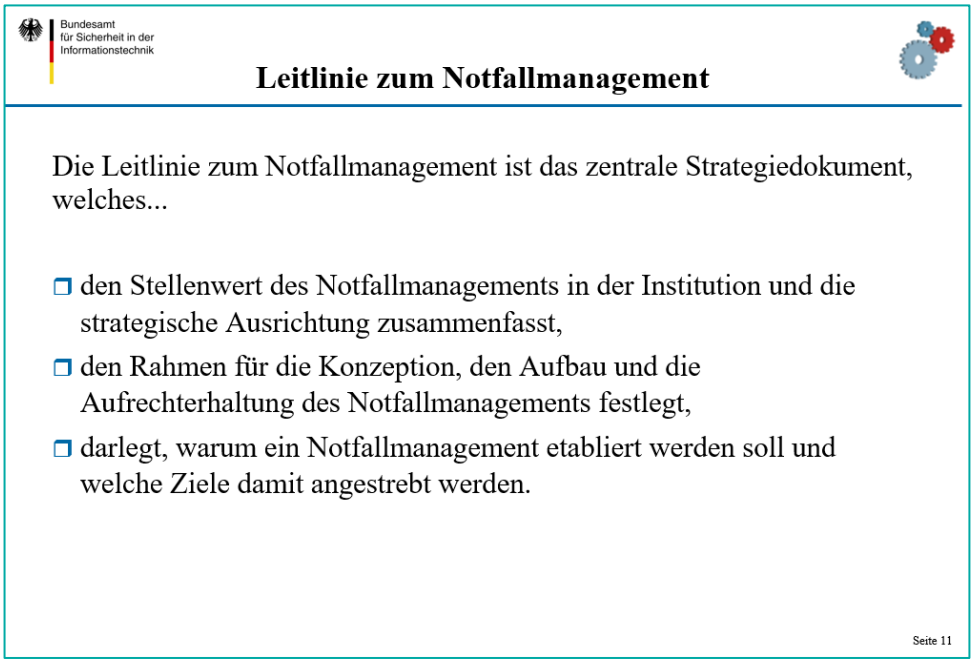


Abbildung 2: Leitlinie zum Notfallmanagement (Quelle: BSI [5])

Zur Entwicklung der Leitlinie gibt das BSI im Rahmenwerk [5] u. a. folgendes vor:

- Die Koordination der Entwicklung und Abstimmung der Leitlinie wird vom Notfallbeauftragten übernommen.
- Die Rahmenparameter des Notfallmanagements werden durch die Institutionsleitung festgelegt.
- Der Notfallbeauftragte zieht ggf. weitere Ansprechpartner für die Entwicklung heran.
- In die Abstimmung sollten möglichst viele Bereiche der Institution einbezogen werden, um die breite Akzeptanz des Ergebnisses zu sichern.

Als mögliche Bereiche / Abteilungen, die bei der Entwicklung der Leitlinie einbezogen werden sollten, werden im Rahmenwerk [5] die Folgenden genannt: Personalvertretung, interne Revision und Risikomanagement.

Darüber hinaus sollten jedoch auch möglichst viele „Stakeholder“ innerhalb und auch außerhalb des Unternehmens berücksichtigt werden, die von einem möglichen Notfall betroffen sein können bzw. bei dessen Vermeidung oder Behandlung einzubeziehen sind. Im Bereich der Energieversorgung steht ein Unternehmen und seine Leistungserbringung vielfach in Abhängigkeitsbeziehungen zu anderen Versorgungsunternehmen sowie zu Lieferanten und Dienstleistern. Diese sollten schon bei der Etablierung des Notfallmanagements so intensiv wie möglich eingebunden werden bis hin zur gegenseitigen Abstimmung der jeweiligen Notfallmanagement-Systeme.

Weitere relevante Stakeholder, die ggf. ebenfalls einbezogen werden sollten, sind z. B. Anteilseigner, Investoren, Versicherer, Aufsichtsbehörden und Branchenverbände.

Nach Fertigstellung der Leitlinie zum Notfallmanagement ist es die Aufgabe der Unternehmensleitung, ihre Zustimmung zu den Aussagen der Leitlinie zu bekunden, sie in Kraft zu setzen, die entsprechende Verantwortung zu übernehmen, und dies – zusammen mit dem Inhalt der Leitlinie – unternehmensweit zu kommunizieren.

3 Inhalte einer Leitlinie zum Notfallmanagement

Die folgenden Unterkapitel behandeln Aspekte des Notfallmanagements, die in einer Leitlinie thematisiert werden sollten. Die Ausführungen brauchen in der Leitlinie nur so ausführlich zu sein, dass die relevanten Festlegungen und Regelungen eindeutig ersichtlich sind. Einzelheiten werden dann in den weiteren Dokumenten zum Notfallmanagement – z. B. Risikoanalyse, Notfallvorsorgekonzept, Notfallhandbuch – dargestellt.

3.1 Definition des Notfallmanagements

Zum gemeinsamen Verständnis von Zielsetzung und organisatorischer Einordnung des Notfallmanagements sollten in der Leitlinie die folgenden Aspekte beschrieben werden:

Bedeutung des Begriffs „Notfallmanagement“

Hier können ggf. auch Begriffe wie „Continuity Management“ / „Business Continuity Management (BCM)“ verwendet werden, abhängig z. B. vom Grad der Orientierung am aktuellen BSI-Standard (Standard 100-4 [4] bzw. demnächst Standard 200-4), aber auch daran orientiert, welcher Begriff im Unternehmen bzw. im geschäftlichen Umfeld üblicherweise verwendet wird. Wichtig für eine gute Kommunikation ist eine einheitliche Begriffsverwendung aller am Notfallmanagement unmittelbar Beteiligten sowie aller Unternehmensmitarbeiter und Stakeholder. Hierzu kann auch eine präzise Verwendung des Begriffs „Notfall“ beitragen, s. u. in Kapitel 3.1.1.

Aufgaben und Kompetenzen des Notfallmanagements

Das BSI schreibt selbst hierzu: „Ziel des Notfallmanagements ist es, sicherzustellen, dass wichtige Geschäftsprozesse selbst in kritischen Situationen nicht oder nur temporär unterbrochen werden und die wirtschaftliche Existenz der Institution auch bei einem größeren Schadensereignis gesichert bleibt.“ (BSI-Standard 100-4 [4]). Bezogen auf die Energiedomäne sollte insbesondere der Stellenwert der Versorgungssicherheit bezogen auf eigene Leistungsverpflichtungen als auch abhängiger Dienstleister thematisiert werden.

Die Themen Versorgungssicherheit und Schwarzstartfähigkeit werden in diesem Dokument nicht behandelt.

Die Verbindung bzw. Kombination von Themen des Notfallmanagements aus IT-technischer Sicht sowie aus physikalischer Sicht werden im Ergebnisdokument AS 12.2.22 „Gap-Analyse“ [8] in Kapitel 3.4 als Thema, das für die Zukunft wichtig ist und für das Lösungen gefunden werden müssen, kurz erörtert.

Schnittstellen zu verwandten Aufgabenbereichen

Hier ist zunächst darzustellen, zu welchen Aufgabenbereichen im Unternehmen Schnittstellen bestehen bzw. bestehen sollen, aus denen sich Zusammenarbeit und Abstimmungsbedarf bei Aufgaben des Notfallmanagements ergeben. Zu diesen Aufgabenbereichen gehören insbesondere Sicherheitsmanagement, Incident Handling, Krisenmanagement, Risikomanagement und ggf. auch Business Continuity Management, sofern das Notfallmanagement nicht einen Teilbereich des BCM bildet.

3.1.1 „Notfall“ – Definition und Abgrenzung

Es kann ggf. hilfreich sein, den Begriff des Notfalls von ähnlichen Begriffen abzugrenzen: Sicherheitsvorfälle werden im Incident Handling (IH) nach ihrer Schwere bzw. Tragweite eingestuft. Zur höchsten Kategorie „hoch“ gehören solche Vorfälle, durch die die Funktionsfähigkeit des gesamten Unternehmens, insbesondere die Erfüllung der Kernaufgaben, gefährdet ist. Es sind z. B. viele wichtige Systeme und Datenbestände betroffen. Weitere Infrastrukturen (z. B. vor- und nachgelagerte Netzbetreiber, Wasserversorgung) werden an der Erfüllung ihrer Kernaufgaben so stark gehindert, dass sie sie nicht mehr erfüllen können. In besonders schweren Fällen, in denen durch Auswirkungen auf die Verfügbarkeit z. B. Gefahren für Leib und Leben eintreten können, wird ggf. die Entscheidung getroffen, dass es sich um einen Notfall handelt und die entsprechenden Maßnahmen einzuleiten sind.

Wenn ein Notfall sich zur existenzbedrohenden Krise verschärft, ist eine Eskalation zum Krisenmanagement erforderlich, siehe BSI-Standard 100-4 [4],

3.2 Geltungsbereich des Notfallmanagements

Der Geltungsbereich des Notfallmanagements sollte möglichst das ganze Unternehmen umfassen. Ähnlich wie bei den Informationsverbünden/Scopes eines ISMS kann es jedoch auch Gründe geben, ein Notfallmanagement für einzelne Standorte oder Geschäftsprozesse/Abteilungen zu etablieren, wenn deren Bedeutung, Abgrenzbarkeit und Größe hierfür jeweils ausreichen.

3.3 Stellenwert des Notfallmanagements für das Unternehmen

Der Stellenwert des Notfallmanagements für das Unternehmen bemisst sich u. a. daran, welche Unternehmensziele in kritischen Situationen in welchem Ausmaß gefährdet sind. Bei der Energieversorgung hat neben wirtschaftlichen Zielen vor allem die Versorgungssicherheit eine hohe Priorität, und entsprechend kann ggf. dargestellt und begründet werden, dass sich das Notfallmanagement besonders auf deren Sicherstellung bezieht.

3.4 Zielsetzung und Kernaussagen der Notfallstrategie

Der Leitfaden sollte grundsätzliche Aussagen zur Notfallstrategie treffen, so dass sich Organisation und Umsetzung des Notfallmanagements daran ausrichten können. Dabei ist zu berücksichtigen, dass im Bereich der Energieversorgung – anders als in anderen Branchen wie etwa Banken und Handel – die Priorisierung der Grundwerte der Informationssicherheit evtl. eine Besonderheit aufweist: Verfügbarkeit und Integrität von Informationen – z. B. Informationen zur Netzsteuerung – können Szenario-bezogen noch höher, also noch kritischer bzw. schützenswerter, eingestuft sein als deren Vertraulichkeit. Siehe hierzu auch die Ergebnisse aus Arbeitsschritt AS 12.2.8 „Schutzbedarfsfeststellung“ [6]. In der Leitlinie zum Notfallmanagement ist darzustellen:

- Geschäftsziele, die durch das Notfallmanagement geschützt werden sollen
- Relevante Schadensszenarien, insbesondere solche, die ggf. existentiell bedrohlich sind, wie z. B.
    - Finanzieller Schaden
    - Beeinträchtigung der Aufgabenerfüllung
    - Verstoß gegen Gesetze, Vorschriften, Verträge
    - Image-Schaden
    - Beeinträchtigung der persönlichen Unversehrtheit
    - Beeinträchtigung der Versorgungssicherheit
- Grundsätzliche Risikobereitschaft bzw. Risikoakzeptanz des Unternehmens
- Ziele mit höchster Priorität bei der Behandlung von Notfällen (z. B. Leib & Leben, Kontinuität von …)

Die Aufgabe des Notfallmanagements ist es, dafür zu sorgen, dass das Unternehmen hinreichend auf Notfallsituationen vorbereitet ist, die existenzgefährdende Auswirkungen haben können. Neben dem Fortbestand des Unternehmens und der Kontinuität der allgemeinen Aufgabenerfüllung sind wesentliche Zielsetzungen des Notfallmanagements im Bereich der Energieversorgung die Abwehr von Einschränkungen des Energieflusses – auch zu verbundenen Unternehmen – und die Sicherstellung der Versorgung betroffener Bevölkerungsanteile.

> Formulierungsvorschlag:
> „Dies erfordert zum einen, dass wir vorbeugende Maßnahmen zum Schutz gegen die relevanten Gefährdungen umsetzen, zum anderen, dass wir geeignete Vorkehrungen und Pläne entwickeln, um auch in Notfällen und kritischen Situationen handlungsfähig zu sein und mögliche Schäden begrenzen zu können.“

Zu den strategischen Kernaussagen einer Leitlinie zum Notfallmanagement gehört auch eine Erklärung der Unternehmensleitung zur Geschäftsstrategie, zur Unterstützung des Notfallmanagements und zur angemessenen Bereitstellung von Ressourcen.

> Formulierungsvorschlag:
> „Die Geschäftsführung unterstützt die Zielsetzung für das Notfallmanagement und stellt daher angemessene Ressourcen für die erforderlichen Planungsprozesse zur Verfügung. Wir sind außerdem bestrebt, in unserer Geschäftsstrategie solche Aktivitäten zu vermeiden, die ein unvertretbares Risiko bedeuten.“

3.5 Vorgehensmodell für das Notfallmanagement

In der Leitlinie zum Notfallmanagement wird festgelegt, an welchem Vorgehensmodell es sich orientieren soll, z. B. durch einen Verweis auf den BSI-Standard 100-4 [4]. Ferner wird eine allgemeine Erklärung zum planmäßigen Vorgehen gegeben. Letztere sollte umfassen:

- Erarbeitung der Notfallvorsorgekonzepte für alle existenziell wichtigen Prozesse mit Verweis, wo diese konkret und im Detail ausgeführt werden.
- Durchführung von Risikoanalyse und Business Impact Analyse für diese Prozesse mit Verweis, wo diese konkret und im Detail ausgeführt werden.

Sofern bereits verwendbare Ergebnisse aus Prozess- und Asset-Dokumentation (z. B. Strukturanalyse im ISMS), Konfigurations-, Change- und Risiko-Management vorliegen, kann auf diese verwiesen werden.

3.6 Verantwortlichkeiten und Pflichten

In der Leitlinie zum Notfallmanagement werden die zugehörigen Rollen und Zuständigkeiten mit den jeweiligen Berichtspflichten beschrieben. Dies dient sowohl der Zuordnung von Aufgaben innerhalb des Notfallmanagements als auch der Orientierung im Unternehmen, z. B. für Prozessverantwortliche mit Schnittstellen zum Notfallmanagement.

Rollen

Die folgenden Rollen sind hier mindestens vorzusehen:

- Notfallbeauftragter
  Der Notfallbeauftragte hat die Prozessverantwortung für das Notfallmanagement, er handelt in Abstimmung mit dem Informationssicherheitsbeauftragten (ISB).

- Informationssicherheitsbeauftragter (ISB)
  Der ISB wird bei allen strategischen Entscheidungen zum Notfallmanagement einbezogen.

- Prozessverantwortlicher
  Dieses Mitglied der Unternehmensleitung trägt als Prozesseigentümer die Verantwortung für das Notfallmanagement.

Berichtspflichten

Bei allen Sicherheitsvorfällen sind alle betroffenen internen Stellen zeitnah zu informieren, ggf. unter Einbeziehung von Datenschutzbeauftragtem, Mitarbeitervertretung und Juristen; dies gilt daher auch für Notfälle. Sollte sich herausstellen, dass ein Sicherheitsvorfall (hier: Notfall) in den Auswirkungen nicht nur auf das Unternehmen beschränkt ist, muss zur Schadensminimierung eine Benachrichtigung der evtl. betroffenen Stellen erfolgen.

Für erhebliche IT-Störungen im Betrieb der „Kritischen Infrastrukturen“ [5] (KRITIS) sieht § 8b BSIG [2] unter anderem eine Meldepflicht für die KRITIS-Betreiber an das BSI vor, damit organisationsübergreifende IT-Störungen durch Warnungen oder Absicherungshinweise des BSI an andere KRITIS-Betreiber verhindert oder abgemildert werden können. Nähere Hinweise dazu, was unter einer erheblichen IT-Störung zu verstehen ist, sowie zum Meldeweg finden sich auf der entsprechenden Homepage[6] des BSI, von der auch die folgende Abbildung zu den Meldekriterien stammt.

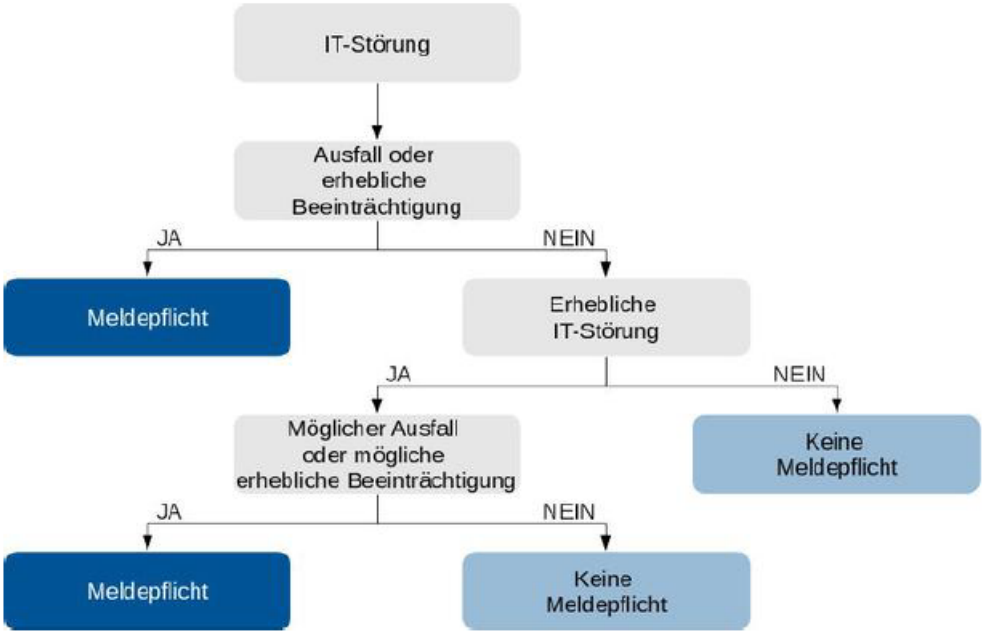


Abbildung 3: KRITIS: Meldekriterien für IT-Störungen (Quelle: BSI, Link siehe Fußnote)

3.7 Aufrechterhaltung und Weiterentwicklung des Notfallmanagements

Die Unternehmensleitung ist verantwortlich und verpflichtet sich entsprechend, das Notfallmanagement kontinuierlich zu optimieren. Hierzu gehören

[5] Organisationen oder Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden. Hierzu gehört u. a. der Sektor „Energie“.

[6] https://www.bsi.bund.de/DE/Themen/KRITIS/IT-SiG/Neuregelungen_KRITIS/Meldepflicht/meldepflicht_node.html

- Regelmäßige allgemeine Überprüfung von Organisation, Maßnahmenumsetzung und Dokumentation des Notfallmanagements mit Angabe von Zeiträumen und Verantwortlichkeiten.
  Hierzu kann z. B. eine Überprüfung alle 2 Jahre durch externes Audit beitragen.
- Durchführung von Tests und Übungen zur Überprüfung der Wirksamkeit des Notfallmanagements und zur Identifikation von Verbesserungsmöglichkeiten, ebenfalls mit Angabe von Zeiten / Zeiträumen und Verantwortlichkeiten.

Hier können ggf. auch weitere Aussagen zur Aufsicht und zur Erfolgskontrolle des Notfallmanagements getroffen werden.

3.8 Zu beachtende Gesetze, Richtlinien und Vorschriften

Die zu beachtenden Gesetze, Richtlinien und Vorschriften hängen jeweils von der Art des Unternehmens und dem Geschäftsfeld bzw. der Branche ab. Relevant für den Bereich der Energieversorgung bzw. KRITIS: Siehe im Hauptdokument [*hier den Verweis zum Ergebnisdokument AS 12.2.21 – Hauptdokument nach dessen Fertigstellung ergänzen*.]

Speziell zum Notfallmanagement sind zu beachten: Siehe im Hauptdokument *[hier den Verweis zum Ergebnisdokument AS 12.2.21 – Hauptdokument nach dessen Fertigstellung ergänzen.]*

3.9 Übernahme der Verantwortung durch die Unternehmensleitung

Die Übernahme der Verantwortung durch die Unternehmensleitung wird durch die explizite Freigabe der Leitlinie zum Notfallmanagement mit Unterschrift dokumentiert.

Für die regelmäßige – hierzu sollte das Zeitintervall angegeben werden – sowie die anlassbezogene Fortschreibung der Leitlinie ist der Notfallbeauftragte verantwortlich. Anlässe können z. B. aus Änderungen von Rahmenparametern (Technologien, Bedrohungsszenarien, etc.), Geschäftszielen, Strategien und Aufgaben resultieren. Die Leitlinie ist dann jeweils erneut durch die Unternehmensleitung freizugeben.

4 Bezugsdokumente

Nr.	Bezeichnung	Inhalt	Link / Ablageort / Datei
1	**BSI IT-Grundschutz**	**BSI-Standard 200-1**: Managementsysteme für Informationssicherheit (ISMS), Version 1.0, Stand 2017-10 **BSI-Standard 200-2**: IT-Grundschutz-Methodik, Version 1.0, Stand 2017-10. **BSI-Standard 200-3**: Risikoanalyse auf der Basis von IT-Grundschutz, Version 1.0, Stand 2017-10. **IT-Grundschutz-Kompendium** 2. Edition 2019	https://www.bsi.bund.de/
2	**BSI-Gesetz**	**Gesetz über das Bundesamt für Sicherheit in der Informationstechnik**	https://www.bsi.bund.de/DE/DasBSI/Gesetz/gesetz_node.html
3	**Ergebnisdokument AS 12.2.16**	„Leitlinie zur Informationssicherheit“	enera Sharepoint: 20170712_enera_Leitlinie zur IS_v1.1.docx
4	**BSI-Standard 100-4**	**BSI-Standard 100-4:** Notfallmanagement, Version 1.0, Stand 2008	https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/BSI-Standard_1004.pdf
5	**Umsetzungsrahmenwerk Notfallmanagement**	**Umsetzungsrahmenwerk zum Notfallmanagement** nach BSI-Standard 100-4 Version 1.0, Stand 2013	https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzStandards/Umsetzungsrahmenwerk/umra.html
6	**Ergebnisdokument AS 12.2.8**	„Schutzbedarfsfeststellung“	enera Sharepoint: 20190301_AS12.2.8_Schutzbedarfsfeststellung_V1.01.docx
7	**Ergebnisdokument AS 12.2.19**	„Incident Handling (IH“	enera Sharepoint: 20190703_AS12.2.19_Incident Handling_V0.02.docx
8	**Ergebnisdokument AS 12.2.22**	„Gap-Analyse“	enera Sharepoint: 2019-12-19_AS12.2.22_Gap-Analyse_v015.docx

Tabelle 1: Bezugsdokumente

5 Abbildungsverzeichnis

Abbildung 1: Notfallmanagement initiieren (Quelle: BSI [5]) 7
Abbildung 2: Leitlinie zum Notfallmanagement (Quelle: BSI [5]) 8
Abbildung 3: KRITIS: Meldekriterien für IT-Störungen (Quelle: BSI, Link siehe Fußnote) 13

6 Tabellenverzeichnis

Tabelle 1: Bezugsdokumente 15

Ergebnisdokument AS 12.2.22

„Gap-Analyse“

Autoren:

Christine Rosinger (OFFIS, AS12.2.22-Verantwortliche), Konrad Rosmus (IABG), Alexandra Quirin (IABG), Rolf Apel (Siemens), Reinhard Schwarz (IESE)

26.03.2021

Gefördert durch:

Bundesministerium
für Wirtschaft
und Energie

aufgrund eines Beschlusses
des Deutschen Bundestages

Historie des Dokuments

Version	Datum	Name	Änderungen	Dateiname
0.1	09.10.2018	Christine Rosinger, OFFIS	Datei erstellt, Gliederung und erste Inhalte.	2018-10-09_AS12.2.22_Gap-Analyse_Stichpunkte.docx
0.2	19.10.2018	Konrad Rosmus, IABG	Kap. 3.3 ISMS i. Zshg. mit dem IT-Sicherheitskatalog formuliert	2018-10-19_AS12.2.22_Gap-Analyse_Stichpunkte.docx
0.3	23.10.2018	Christine Rosinger, OFFIS	Zusammenführung der zwei bestehenden Dokumente & kleine Anpassungen/Erweiterungen	2018-10-23_AS12.2.22_Gap-Analyse.docx
0.4	01.11.2018	Christine Rosinger, OFFIS	Kleine Ergänzungen	2018-11-01_AS12.2.22_Gap-Analyse.docx
0.5	20.02.2019	Rolf Apel, Siemens	Kapitel 3.7 und 3.8	2019-02-20_AS12.2.22_Gap-Analyse_v05.docx
0.6	01.03.2019	Christine Rosinger, OFFIS	Kapitel 3.7 und 3.8 ergänzt	2019-03-01_AS12.2.22_Gap-Analyse_v06.docx
0.7	02.04.2019	Christine Rosinger, OFFIS	Kleine Änderungen zu Kapitel 3.7 und 3.8 (Kommentare M. Uslar)	2019-04-02_AS12.2.22_Gap-Analyse_v07.docx
0.8	23.04.2019	Christine Rosinger, OFFIS	Begriffsdefinition Gap-Analyse überarbeitet (Input von Alexandra Quirin, IABG)	2019-04-23_AS12.2.22_Gap-Analyse_v08.docx
0.9	26.04.2019	Christine Rosinger, OFFIS	Begriffsdefinition angepasst	2019-04-26_AS12.2.22_Gap-Analyse_v09.docx
0.10	12.06.2019	Christine Rosinger, OFFIS	Absatz in Abschnitt 2 ergänzt	2019-06-12_AS12.2.22_Gap-Analyse_v010.docx
0.11	08.08.2019	Rolf Apel, Siemens	Ergänzungen zu Abschnitt 3.4 und 3.5	2019-08-08_AS12.2.22_Gap-Analyse_v011.docx
0.12	13.08.2019	Christine Rosinger, OFFIS	Abschnitt 3.4 und 3.5 korrekturgelesen und ergänzt	2019-08-13_AS12.2.22_Gap-Analyse_v012.docx

Version	Datum	Name	Änderungen	Dateiname
0.13	12.12.2019	Konrad Rosmus, IABG	Abschnitt 3.4: Zusammenhang der Grundwerte umgearbeitet	20191212_AS12.2.22_Gap-Analyse_v013.docx
0.14	13.12.2019	Christine Rosinger, OFFIS	Abschnitt 3.4 abgenommen und Überarbeitungen angenommen	20191213_AS12.2.22_Gap-Analyse_v014.docx
0.15	19.12.2019	Christine Rosinger, OFFIS	Abschnitt 3.1 und 3.6 begonnen, Tabelle und Abkürzungsverzeichnis überarbeitet	2019-12-19_AS12.2.22_Gap-Analyse_v015.docx
0.16	24.07.2020	Christine Rosinger, OFFIS	Kommentare und Ergänzungen von Reinhard Schwarz eingearbeitet: Abschnitte 3.8 und 3.10 ergänzt; Abkürzungsverzeichnis und Literaturverzeichnis ergänzt	2020-07-24_AS12.2.22_Gap-Analyse_v016.docx
0.17	23.03.2021	Christine Rosinger, OFFIS	Fehlende Abschnitte ergänzt und nahezu finalisiert	2021-03-23_AS12.2.22_Gap-Analyse_v017.docx
1.0	26.03.2021	Christine Rosinger	Feedback von Ulrike und Marie eingearbeitet und finalisiert.	2021-03-26_AS12.2.22_Gap-Analyse_v1_0.docx

Inhalt

Abkürzungsverzeichnis **5**

1 Einleitung **7**

1.1 Ausgangslage und Problemstellung 7

1.2 Gliederung 7

2 Einordnung und Begrifflichkeiten **8**

2.1 Begriff Gap-Analyse 8

2.2 Einordnung im Projekt 9

3 Identifizierte Lücken und Beseitigungsstrategien **9**

3.1 Methodik nach NIST IR 7628 erweitern 10

3.2 Lücken in Regularien aus AS 12.2.1 12

3.3 Zertifizierung eines ISMS: Nach IT-Grundschutz ermöglichen 12

3.4 Zusammenführung Notfallmanagement 13

3.5 Informationssicherheit versus Funktionssicherheit 16

3.6 Informationssicherheitsmanagement bei vielen Partnern 16

3.7 Durchsetzen kontinuierlicher Informationssicherheit 18

3.8 Use-Case-Methodik nach IEC 62559 für Sicherheitsanalysen 20

3.9 Erstellung von Informationsobjekt-Katalogen 22

3.10 Goal Structuring Notation für ein nachvollziehbares Sicherheitsdesign 23

3.11 Grundschutzprofil z. B für Smart Home 25

4 Zusammenfassung und Ausblick **25**

Literaturverzeichnis **28**

Abbildungsverzeichnis **29**

Tabellenverzeichnis **29**

Abkürzungsverzeichnis

Abkürzung	Bedeutung
ACER	Agency for the Cooperation of Energy Regulators
AP	Arbeitspaket
AS	Arbeitsschritt
BMWi	Bundesministerium für Wirtschaft und Energie
BNetzA	Bundesnetzagentur
BSI	Bundesamts für Sicherheit in der Informationstechnik
BSIG	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik
BSI-KritisV	Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz
CIA	*Schutzziele:* Confidentiality (Vertraulichkeit), Integrity (Integrität) und Availabilitiy (Verfügbarkeit)
CLS	Controllable Local System
DAkkS	Deutsche Akkreditierungsstelle
DG ENER	Die Generaldirektion der Europäische Kommission für Energie
DIN	Deutsches Institut für Normung
DKE	Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE
EMT	Externer Marktteilnehmer
ENTSO-E	European Network of Transmission System Operators for Electricity
GSN	Goal Structuring Notation
GVB	Gesamtvorhabensbeschreibung
HL	High-Level (häufig in Kombination: High-Level-Informationsobjekte, auch HL-InfoObjekte)
IEC	International Electrotechnical Commission
IEC SyC SE	IEC System Committee Smart Energy
IKT	Informations- und Kommunikationstechnik
IR	Interagency Report
ISMS	Informationssicherheitsmanagementsystem

Abkürzung	Bedeutung
ISO	Internationale Organisation für Normung
MSB	Messstellenbetreiber
NERC CIP	North American Electric Reliability Corporation Critical Infrastructure Protection
NIST	National Institute of Standards and Technology
NWIP	New Work Item Proposal
OT	Operation Technology
PM	Projektmanagement
SGAM	Smart Grid Architecture Model
SINTEG	Schaufenster intelligente Energie – Digitale Agenda für die Energie-wende
SMGW	Smart Meter Gateway
TAP	Teilarbeitspaket
TVB	Teilvorhabensbeschreibung
UC	Use Case
UCMR	Use Case Management Repository
VDE	Verband der Elektrotechnik Elektronik Informationstechnik e. V.
WG	Working Group

Ergebnisdokument AS 12.2.22

„Gap-Analyse“

1 Einleitung

Diese Einleitung stellt die Ausgangslage und Problemstellung für diesen Arbeitsschritt (AS) dar und erläutert die weitere Gliederung des Dokuments.

1.1 Ausgangslage und Problemstellung

Enera ist eins der fünf durch das Bundesministeriums für Wirtschaft und Energie (BMWi) geförderten Projekte des Förderprogramms „Schaufenster intelligente Energie – Digitale Agenda für die Energiewende“ (SINTEG)[1]. Im Projekt werden Lösungen zu den drei Themenschwerpunkten Netz, Markt und Daten in der Modellregion im Nordwesten Niedersachsens entwickelt und erprobt. Das **Arbeitspaket (AP) 12** innerhalb dieses Projekts beschäftigt sich mit der informationstechnischen Entwicklung der enera Gesamtarchitektur inklusive eines Informationssicherheitskonzepts.

Das **Teilarbeitspaket (TAP) 12.2** befasst sich mit dem Informationssicherheitskonzept. Der dazugehörige **Arbeitsschritt (AS) 12.2.22** mit dem Titel „Gap-Analyse“ setzt sich innerhalb dieses TAPs damit auseinander, welche Lücken bei der Entwicklung eines Informationssicherheitskonzepts für die Energiedomäne im TAP 12.2 im Rahmen der Projektlaufzeit aufgefallen sind und entwickelt, wenn möglich, entsprechende Lösungsvorschläge für die identifizierten Lücken. Die Ergebnisse dieses Arbeitsschritts werden innerhalb dieses Dokuments festgehalten.

1.2 Gliederung

Das weitere Dokument gliedert sich wie folgt: Abschnitt 2 gibt eine Einordnung zum Thema Gap-Analyse und erläutert die Begrifflichkeiten Gap-Analyse und Informationssicherheitsmanagementsystem (ISMS). In Abschnitt 3 werden die identifizierten Lücken aufgelistet und beschrieben. Weiterhin werden, wenn möglich, für die identifizierten Lücken jeweils Lösungsvorschläge dargestellt. Abschließend gibt Abschnitt 4 eine Zusammenfassung.

---

[1] Siehe auch die Seite des SINTEG-Förderprogramms auf der Homepage des BMWi https://www.bmwi.de/Redaktion/DE/Artikel/Energie/sinteg.html.

2 Einordnung und Begrifflichkeiten

Dieses Kapitel definiert in Abschnitt 2.1 zunächst den Begriff Gap-Analyse und beschreibt danach in Abschnitt 2.2 die Einordnung des Arbeitsschritts AS 12.2.22 „Gap-Analyse“ im Projekt enera.

2.1 Begriff Gap-Analyse

Bei der Gap-Analyse (engl.: gap = Lücke) werden Lücken identifiziert, analysiert und mögliche Behebungsstrategien aufgezeigt. Die Gap-Analyse hat viele Anwendungsbereiche und kann u.a. in der Betriebswirtschaftslehre als Managementinstrument dienen oder als Instrument in der Standardisierung verwendet werden, um fehlende Aspekte eines Standards oder einer Norm aufzudecken.

In der Betriebswirtschaftslehre werden beispielsweise die Abweichungen zwischen unterschiedlichen Entwicklungsverläufen eines Unternehmens identifiziert, um die Lücken zwischen den Verläufen darzustellen. Damit sollen für die Zukunft Lücken zwischen dem aktuellen Basisgeschäft und alternativen Entwicklungen ermittelt und dargestellt werden. Als Folge davon werden dann Veränderungen und Anpassungen der Unternehmensstrategie vollzogen, die wiederum die Abweichungen beseitigen oder minimieren. Dabei besteht die Gap-Analyse aus der Darstellung von Abweichungen, deren Interpretation sowie Vorschlägen zur Schließung der identifizierten Lücken.

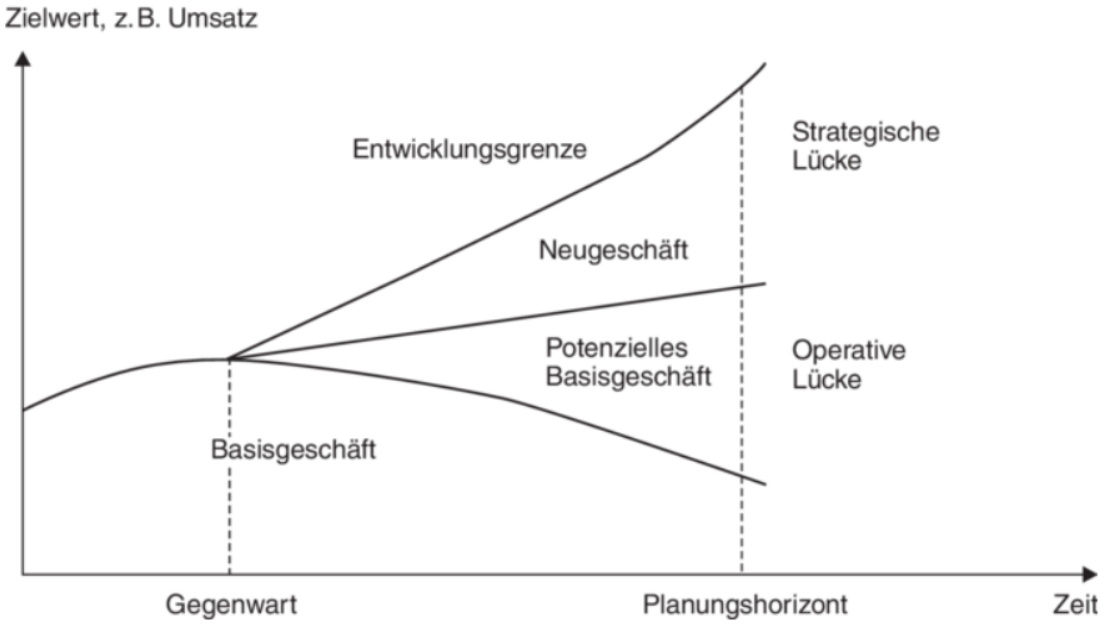


Abbildung 1: Darstellung Gap-Analyse [GABL 18]

Die Darstellung hierfür kann in einem zweidimensionalen Koordinatensystem erfolgen. Auf der Abszisse wird die Zeit aufgetragen, auf der Ordinate der entsprechende Lückenindikator (siehe

Abbildung 1). Die Kurven zeigen die unterschiedlichen Entwicklungen, wodurch die Lücke entsteht. Die Abweichung kann ggf. in einen operativen und strategischen Anteil unterteilt werden.

Darüber hinaus werden mittels Gap-Analyse Lücken von Standards bzw. Normen aufgezeigt, die im jeweils aktuellen Standard noch nicht abgedeckt sind. Weiterhin werden darin mögliche Maßnahmen zur Beseitigung der Abweichungen herausgearbeitet und festgestellt, was zusätzlich geregelt werden muss. Dies erfolgt meist textuell in Dokumentenform.

Insgesamt dient die Gap-Analyse einer groben Darstellung der Lücken zur ersten Interpretation. Das Instrument der Gap-Analyse ist explorativ und wenig differenziert. Externe Entwicklungen werden nicht einbezogen, obwohl diese oft zu dynamischen Veränderungen führen. Die Gap-Analyse basiert auf der Extrapolation von Vergangenheitswerten. Die Gap-Analyse zeigt zunächst nur Lücken und Schwachstellen auf; Handlungsempfehlungen und Maßnahmen zur Schließung der Lücke lassen sich nicht direkt ableiten, sondern sind zu erarbeiten. Zur weiteren Analyse können zusätzliche Instrumente für eine detaillierte Aussage hinzugezogen werden.

2.2 Einordnung im Projekt

Im Rahmen von AS 12.2.22 sind Lücken bei der Etablierung von Informationssicherheit zu identifizieren. Innerhalb der Gesamtvorhabensbeschreibung (GVB) sowie den einzelnen Teilvorhabensbeschreibungen (TVB) der beteiligten Partner sind die Aufgaben dieses AS nicht detailliert beschrieben, so dass die genauen Inhalte für diesen AS im Rahmen des Projekts erst erarbeitet werden mussten. Innerhalb dieses Arbeitsschritts wurden daher Lücken für Informationssicherheitsaspekte im Kontext von enera ermittelt. Diese identifizierten Lücken werden in Kapitel 3 zunächst tabellarisch aufgeführt. Danach wird pro identifizierte Lücke jeweils ein einzelner Abschnitt in der Art gestaltet, dass zunächst die Lücke beschrieben wird und anschließend, wenn möglich, potenzielle Beseitigungsstrategien aufgezeigt werden.

3 Identifizierte Lücken und Beseitigungsstrategien

Dieses Kapitel erläutert Lücken, die während der Arbeiten zu TAP 12.2 ermittelt wurden. An der Identifizierung und Beschreibung der Lücken waren dabei das Analyse- und Testdienstleistungs-Unternehmen IABG, das Fraunhofer-Institut für Experimentelles Software Engineering IESE, das Oldenburger Informatik-Institut OFFIS und der Mischkonzern Siemens als Projektpartner beteiligt. Auf dem Projekttreffen des AP 12 in Ottobrunn am 24.08.2017 wurden bereits mögliche Lücken identifiziert und dokumentiert. Auf einem weiteren AP 12-Treffen in Saarbrücken am 16. und 17.05.2018 wurden die relevanten Lücken festgehalten und in der Folge weiter ergänzt und aktualisiert (siehe Tabelle 1). Diese Lücken werden in den nächsten Abschnitten beschrieben und mögliche Gegenmaßnahmen aufgezeigt.

Abschnitt-Nr.	Relevante Lücken	Verantwortliche	Status	Zeitrahmen
3.1	Methodik nach NIST IR 7628 erweitern	OFFIS	erledigt	✓
3.2	Lücken in Regularien aus AS 12.2.1	Werden in AS 12.2.4 behandelt	Für AS12.2.22 erledigt	✓
3.3Zertifizierung eines ISMS: Nach IT-Grundschutz ermöglichen	Zertifizierung eines ISMS: Nach IT-Grundschutz ermöglichen	IABG	erledigt	✓
3.4	Zusammenführung Notfallmanagement	Siemens, IABG	erledigt	✓
3.5	Informationssicherheit versus Funktionssicherheit	Siemens, IESE	erledigt	✓
3.6	Informationssicherheitsmanagement bei vielen Partnern	OFFIS	erledigt	✓
3.7	Durchsetzen kontinuierlicher Informationssicherheit	Siemens, OFFIS	erledigt	✓
3.8	Use-Case-Methodik nach IEC 62559 für Sicherheitsanalysen	Siemens, OFFIS	erledigt	✓
3.9	Erstellung von Informationsobjekt-Katalogen	Siemens, OFFIS	erledigt	✓
3.10	Goal Structuring Notation für ein nachvollziehbares Sicherheitsdesign	OFFIS, IESE	erledigt	✓
3.11	Grundschutzprofil z. B. für Smart Home	OFFIS, IABG	erledigt	✓

Tabelle 1: Statustabelle identifizierte Lücken (wurde regelmäßig aktualisiert)

3.1 Methodik nach NIST IR 7628 erweitern

Bereits vor Beginn der enera Projektlaufzeit wurde im Rahmen der Arbeiten von OFFIS im Themenfeld Informationssicherheit für das Smart Grid ein Analyseansatz erarbeitet, der auf verschiedenen bestehenden Methoden beruht. Dieser Ansatz ist in Abbildung 2 dargestellt und besteht aus folgenden Schritten:

1. Erfassung von relevanten Anwendungsfällen mit dem UC-Template (UC = Use Case) aus dem Standard IEC 62559.
2. Mapping der Anwendungsfälle mit seinen Akteuren, Schnittstellen und ausgetauschten Informationen auf den Standard NIST IR 7628, der auch auf der rechten Seite der Abbildung dargestellt ist und aus dem US-amerikanischen Raum stammt.
3. Durchführung einer Risikoanalyse des Anwendungsfalls auf dieser Basis, zusammen mit Ansätzen aus dem EU Mandat M / 490.
4. Ermittlung und Zuordnung von Schutzmaßnahmen aus dem NIST IR 7628.
5. Ableitung individueller Empfehlungen bezogen auf den UC.

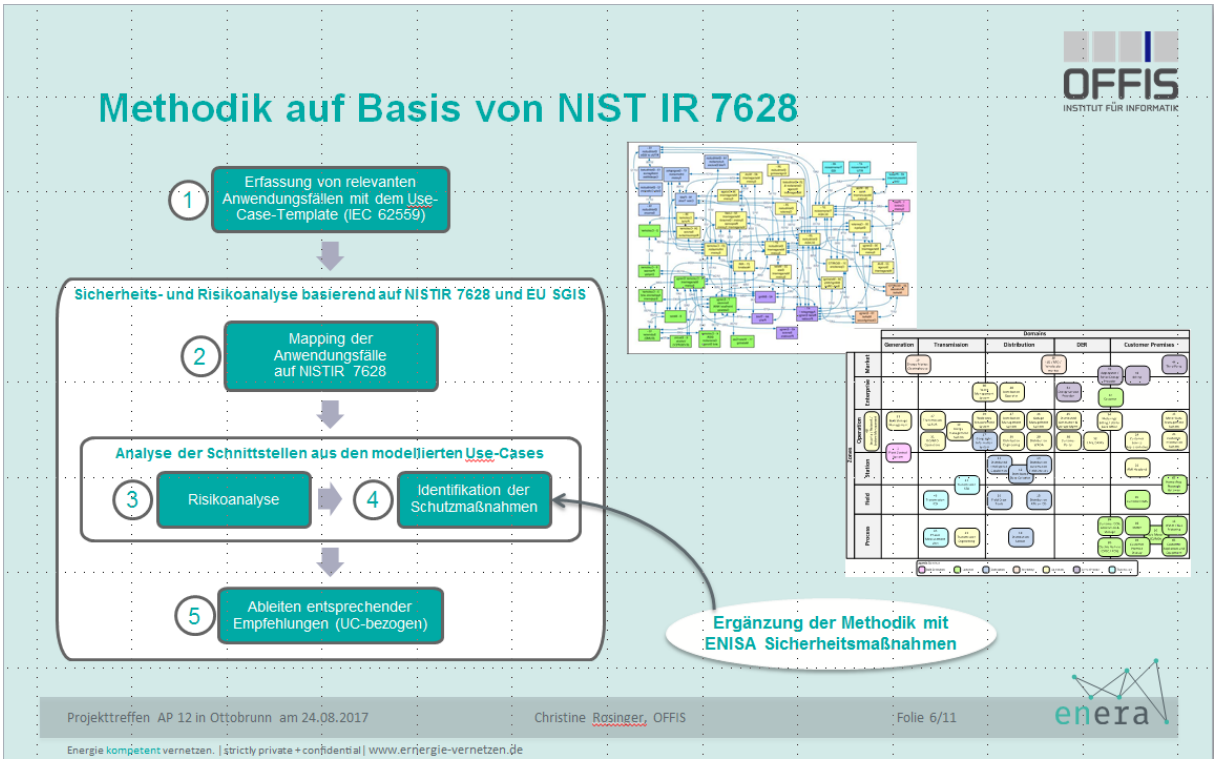


Abbildung 2: Sicherheitsanalyse-Methodik für Smart-Grids basierend auf NIST IR 7628

Da der NIST IR 7628 aus dem US-amerikanischen Raum stammt, sollte diese Methodik im 4. Schritt mit Sicherheitsmaßnahmen, die im europäischen Raum weitreichend akzeptiert sind, erweitert werden. Hierfür wurden die Sicherheitsmaßnahmen aus dem Dokument „ENISA Smart Grid Security Recommendations“ in die Methodik integriert, die folgende Standards beinhaltet: ISO 270xx, IEC 62443 und NERC CIP.

Ende des Jahres 2019 wurde die Richtlinie VDE 0175-110 mit dem Titel „Richtlinie zur IT-Sicherheit und Resilienz für die Smart-Energy-Einsatzumgebung (VDE 0175-110)“ veröffentlicht, die nun auch im europäischen Kontext die NIST IR 7628 Richtlinie verwendet.

Wir empfehlen daher, die Methoden diese Richtlinie nun im europäischen Kontext zu verwenden und bei Bedarf durch weitere relevante Standards zu erweitern.

3.2 Lücken in Regularien aus AS 12.2.1

Die Lücken von Regularien aus AS 12.2.1 „Gesetze, Regularien, Richtlinien, Compliance, Zertifizierungen“ werden im Rahmen von AS 12.2.4 bearbeitet.

3.3 Zertifizierung eines ISMS: Nach IT-Grundschutz ermöglichen

Zum Nachweis, dass die Anforderungen des IT-Sicherheitskatalogs erfüllt werden, hat die Bundesnetzagentur (BNetzA) gemeinsam mit der Deutschen Akkreditierungsstelle (DAkkS) ein eigenes Zertifikat erarbeitet. Das Zertifikat basiert dabei im Wesentlichen auf dem bereits existierenden Zertifikat bzw. Zertifizierungsschema zur ISO/IEC 27001 und ergänzt dieses um die zusätzlichen Anforderungen des IT-Sicherheitskatalogs nach IT-Grundschutz des Bundesamts für Sicherheit in der Informationstechnik (BSI). Darin soll auch der Anwendungsbereich (Scope) spezifiziert werden, um sicherzustellen, dass zumindest die für einen sicheren Netzbetrieb notwendigen Telekommunikations- und Datenverarbeitungssysteme von der Zertifizierung erfasst sind.

Basis für die Zertifizierung muss ein "natives" ISO 27001 Zertifikat sein; ein Zertifikat ISO 27001 auf Basis IT-Grundschutz wird nicht anerkannt. Die BNetzA erklärt dazu: "Bereits bestehende Zertifizierungen nach ISO/IEC 27001, BSI Grundschutz usw. sind daher nicht ausreichend, um die Erfüllung der Anforderungen des IT-Sicherheitskatalogs nachzuweisen.“ [BNA 20].

Diese Erklärung ist aus ISMS-Sicht nicht nachvollziehbar, insbesondere, weil ISO 27001 auf Basis IT-Grundschutz ein höheres Mindestsicherheitsniveau gewährleistet als ISO 27001 nativ. Dies gilt vor allem im technischen Bereich und genau technische Sicherheitsfragen (z. B. Kommunikationsnetze für das Fernwirken) sollten bei der Zertifizierung von Energieversorgern im Vordergrund stehen.

Selbst dadurch, dass in DIN ISO / IEC TR 27019 (DIN SPEC 27019) spezielle Umsetzungsempfehlungen im Bereich der Prozesssteuerung der Energieversorgung beschrieben sind, wird nicht notwendigerweise ein Sicherheitsniveau erreicht, das mindestens dem des IT-Grundschutzes entspricht. Die Umsetzungsempfehlungen lassen sowohl den Planern und Implementierern, als auch den Auditoren viel Ermessensspielraum, so dass nicht ausgeschlossen werden kann, dass technische Maßnahmen nicht ausreichend implementiert sind.

Der Umstand, dass im IT-Grundschutz nicht notwendigerweise eine Risikoanalyse gemacht werden muss, ist ebenso kein nachvollziehbarer Grund, ihn für das ISMS zum Sicherheitskatalog auszuschließen, da Risikoanalysen implizit in den Bausteinen enthalten sind und beim Vorliegen eines erhöhten Schutzbedarfs oder besonderer Technologien oder Einsatzbedingungen zusätzlich vorgesehen sind.

Schließlich sei auch noch darauf hingewiesen, dass andere Zertifizierungen, wie etwa TR-03109-6 SMGWA und TR-03145 Secure CA Operation, der Organisation die Wahl lassen, ob das zu Grunde liegende ISMS nach ISO 27001 oder ISO 27001 auf Basis IT-Grundschutz zertifiziert ist.

Es wird empfohlen, für die Zertifizierung von Energieversorgern nach dem IT-Sicherheitskatalog gemäß § 11 Absatz 1a Energiewirtschaftsgesetz für das zu Grunde liegende ISMS auch eine Zertifizierung gemäß ISO 27001 auf Basis IT-Grundschutz zuzulassen.

Sofern noch nicht durch neue Bausteine des IT-Grundschutz-Kompendiums [BSI 2020] abgedeckt (z. B. IND.1 Betriebs- und Steuerungstechnik, IND.2.1 Allgemeine ICS-Komponente, IND.2.3 Sensoren und Aktoren), können die Umsetzungsempfehlungen DIN ISO / IEC TR 27019 (DIN SPEC 27019) über eine Risikoanalyse mitaufgenommen werden, welche nach dem modernisierten Standard BSI 200-3 erfolgen kann.

3.4 Zusammenführung Notfallmanagement

Das Notfallmanagement im Bereich der Energieversorgung (mit allen Unterthemen) sollte mit dem Notfallmanagement im Bereich Informationsverarbeitung / Informationssicherheit gekoppelt und synchronisiert werden: Dies betrifft auch weitere Managementbereiche, wie z. B. die Behandlung von Sicherheitsvorfällen, oder auch das Testen, sowie die Ausbildung und Sensibilisierung von Personal und eventuell weitere Themenfelder. Allerdings muss man beim Notfallmanagement in Energieversorgungssystemen die – gegenüber der allgemeinen Informationsverarbeitung – unterschiedliche Priorisierung bei der IT-Sicherheit im Auge behalten (siehe auch Abbildung 3). So gilt in der allgemeinen Informationsverarbeitung oftmals die CIA-Priorisierung

1. Confidentiality (Vertraulichkeit)
2. Integrity (Integrität)
3. Availability (Verfügbarkeit)

oder die drei Grundwerte haben zumindest die gleiche Priorität. Im Energieversorgungssystem hingegen dominiert als Ziel die Versorgungssicherheit, also die Versorgung der Allgemeinheit mit Elektrizität. Im Sinne der drei Grundwerte bedeutet dies: Die Verfügbarkeit der für die Aufrechterhaltung der Energieversorgung notwendigen Daten, Anwendungen und Systeme hat

höchste Priorität. Damit spielen z. B. Aspekte wie Notstromversorgung, redundante Kommunikationseinrichtungen, Wartung und dergleichen eine wichtige Rolle bei der IT-Sicherheitsbetrachtung im Energieversorgungssystem.

Die rechtlichen Grundlagen zum Notfallmanagement im Bereich kritischer Infrastrukturen, zu denen auch Teile des Energieversorgungssystems gehören, sind im Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) definiert. Welche Teile des Energieversorgungssystems als kritische Infrastruktur eingestuft werden, regelt die Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-KritisV). Allerdings definieren diese Gesetze und Verordnungen keine Details eines entsprechenden Notfallmanagements.

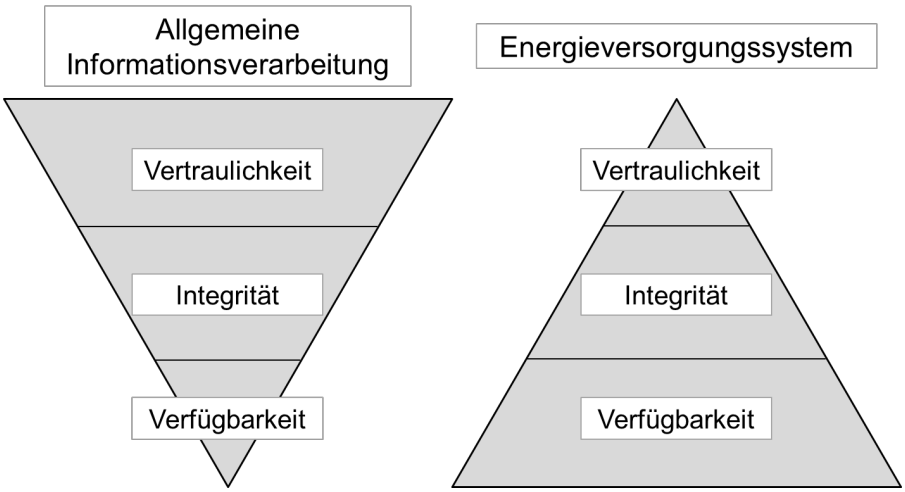
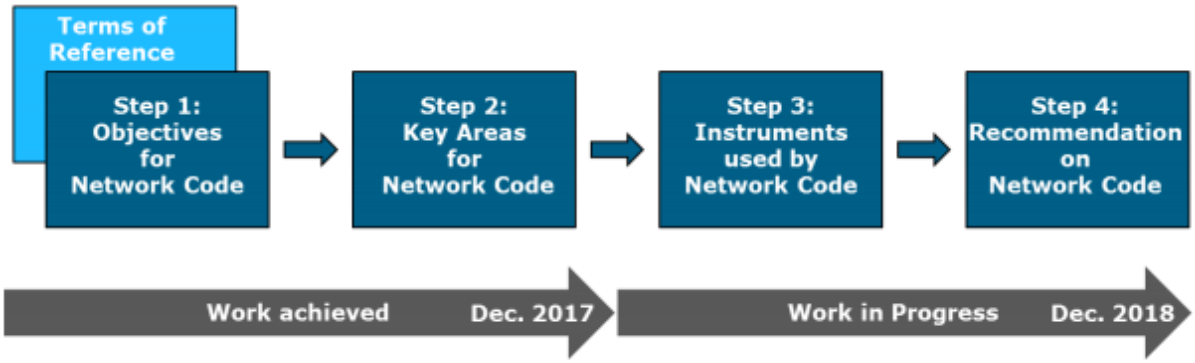


Abbildung 3: Vergleich der Priorisierung von Schutzzielen

Da die Energieversorgung ein grenzüberschreitendes System ist, gibt es auch auf europäischer Ebene Aktivitäten zu diesem Thema. Die Generaldirektion der Europäischen Kommission für Energie (DG ENER) hat im Rahmen der Smart Grid Task Force dazu eine Expertengruppe ins Leben gerufen, die Regulierungsempfehlungen für Datenschutz, Datensicherheit und Cybersicherheit im Smart-Grid-Umfeld erarbeiten soll (Smart Grids Task Force – Expert Group 2 – Cybersecurity). Aus diesen Empfehlungen sollen dann ENTSO-E und ACER Network Codes[2] für Cyber Security erarbeiten. Diese sind dann von den Mitgliedstaaten der EU in nationale Anwendungsregeln umzusetzen. Abbildung 4 gibt einen Überblick über die ursprüngliche Planung der Aktivitäten zu den Network Codes dieser Expertengruppe.

Gemäß Abbildung 5 sollen diese Network Codes neben den technischen Anforderungen an die Systemkomponenten, auch Vorgaben für ein Vorwarnsystem erhalten, um Cyber-Attacken frühzeitig erkennen und Gegenmaßnahmen ergreifen zu können.

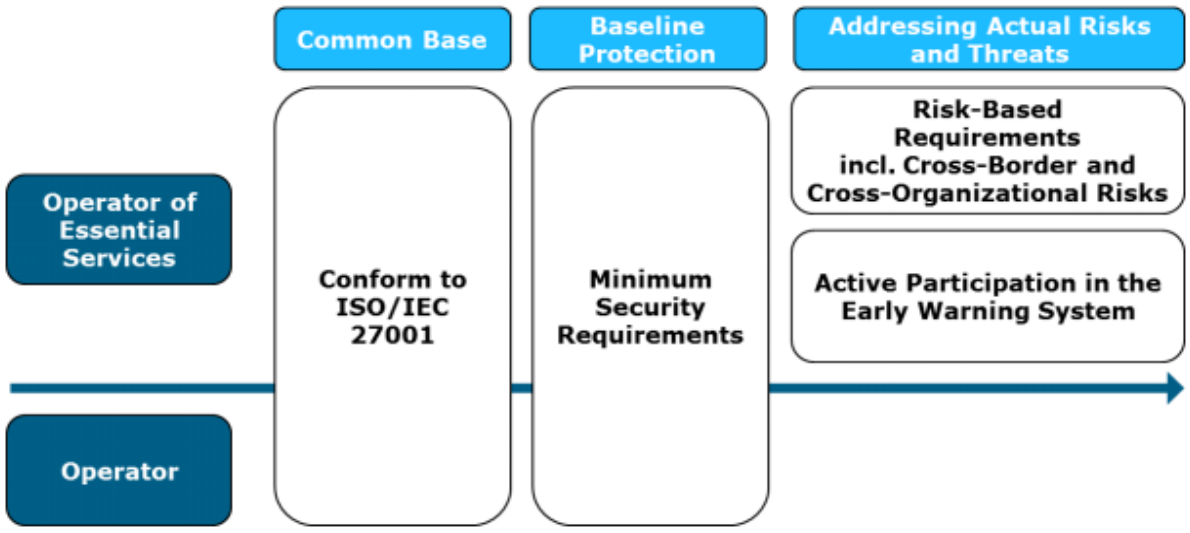
[2] „Die europäischen Network Codes sind eine Sammlung von Regelwerken, die einheitliche Mindestanforderungen für den Netzzugang und Netzbetrieb vorgeben.“ Quelle: https://www.netztransparenz.de/EU-Network-Codes.



[Quelle: https://ec.europa.eu/energy/sites/ener/files/sgtf_eg2_2nd_interim_report_final.pdf]

Abbildung 4: Überblick Analyse und Ansatz für Implementierung

Sollte es trotz aller Maßnahmen zu einem Netzausfall gekommen sein, gilt es, die Energieversorgung wiederaufzubauen. Auch hierfür gibt es auf europäischer Ebene den Network Code on Emergency and Restoration. Darin werden die Prozeduren für den Netzwiederaufbau geregelt und auch die Mindestanforderung an die Kommunikationstechnik definiert (Schwarzstartfähigkeit). Allerdings sind hier die Aspekte des Trends zu immer mehr verteilter Erzeugung noch wenig berücksichtigt.



[Quelle: https://ec.europa.eu/energy/sites/ener/files/sgtf_eg2_2nd_interim_report_final.pdf]

Abbildung 5: Empfohlene Struktur für Network Code bei Cybersicherheit

Zusammenfassend lässt sich sagen, dass das Thema Notfallmanagement in Energieversorgungssystemen noch nicht alle Aspekte der fortschreitenden Energiewende und Digitalisierung berücksichtigt. Hier können auch die im AP12 des enera-Projekts erarbeiteten Ergebnisse sicher einen guten Beitrag leisten.

3.5 Informationssicherheit versus Funktionssicherheit

Wie schon im vorangegangenen Abschnitt beschrieben, unterscheiden sich die Priorisierungen bei der IT-Sicherheit zwischen allgemeiner IT und IT für den Betrieb von Energieversorgungssystemen (siehe auch Abbildung 3), oft auch Operation Technology (OT) genannt. Da durch die fortschreitende Digitalisierung immer mehr Datenaustausch zwischen diesen beiden Welten notwendig wird, z. B. um Asset Management und ähnliche Aufgaben zu unterstützen, muss an den Schnittstellen ein besonderes Augenmerk darauf gelegt werden, wie diese unterschiedlichen Priorisierungen realisiert werden können.

Während in der IT ein Abschalten der externen Kommunikationsverbindungen eine Notfalloption sein kann, würde dies im OT-Bereich zu einem Ausfall der Netzüberwachung und Kontrolle führen und stellt damit keine Handlungsoption dar. Aus diesem Grund und aus Gründen der Verfügbarkeit im Schwarzfall muss bei der sicherheitstechnischen Konzeption der IT-Systeme im Energieversorgungssystem eine saubere Trennung der beiden Welten mit definierten Schnittstellen erfolgen. Im Falle eines Falles können dann durch Trennung an diesen Punkten unterschiedliche Notfallmanagementprozesse für beide Welten umgesetzt werden.

3.6 Informationssicherheitsmanagement bei vielen Partnern

Informationssicherheitsmanagement wird üblicherweise unternehmensweit durchgeführt und nicht wie hier im enera Projekt mit vielen Partnern zusammen. Das heißt, ein Unternehmen legt u. a. fest, in welchem Umfang Informationssicherheit im Unternehmen relevant und umzusetzen ist (dargestellt in der Sicherheitsleitlinie); hierfür trägt das Unternehmen dann die entsprechenden Kosten und Aufwände, sowie ggf. auch die Risiken für bestimmte Bedrohungsszenarien. In bundesgeförderten Forschungsprojekten o. ä. erfolgt die Projektarbeit allerdings unternehmensübergreifend und auch weitgehend gleichberechtigt. Dies führt dazu, dass Informationssicherheitskonzepte im Forschungsprojekt erarbeitet werden, dass aber nicht abschließend vorgeschrieben werden kann, welche Maßnahmen pro Unternehmen genau umzusetzen sind.

Um für dieses Themenfeld, „Informationssicherheit bei vielen Partnern“, Lösungsansätze zu finden, kann man sich in anderen Bereichen umschauen, die ähnliche Themenkomplexe bearbeiten. Sowohl im Bereich Projektmanagement (PM) als auch in den Rechtswissenschaften gibt es Lösungsansätze für dieses Themenfeld. Im enera-Projekt wurden diese zwei parallelen Themenkomplexe in den benannten Bereichen identifiziert und im Folgenden diskutiert:

1. Das Thema „Führen ohne Weisungsbefugnis“ spielt beim PM immer wieder eine Rolle, so dass sich hieraus Problemfelder und Lösungsansätze für den hier behandelten Themenkomplex ableiten lassen. Aus diesem Projektmanagement-Themenfeld können folgende Problemfelder abgeleitet werden, die auch beim Informationssicherheitsmanagement mit vielen Partnern bedacht werden sollten:

- Projektleiter ist nicht unbedingt in der Leitungsebene tätig und für keine oder nicht alle Projektpartner weisungsbefugt, hat daher evtl. keinen direkten Einfluss auf die Verfügbarkeit von Projektmitarbeitern und unklare Verantwortlichkeiten.

  ➔ Für die Erarbeitung und Umsetzung von Informationssicherheitsmaßnahmen bedeutet dies, dass es abgestimmte und gemeinsame Zielvorstellungen zu den relevanten Aspekten sowie ebenfalls gemeinsame und abgestimmte Bereitstellungen von nutzbaren Ressourcen für diese Zwecke geben sollte.

- Förderprojekte haben nicht immer klare Zielvorgaben, daher liegen gerade zu Beginn unklare Ziele vor bzw. die verschiedenen beteiligten Unternehmen verfolgen unterschiedliche Ziele oder haben sogar gegensätzliche Zielvorgaben.

  ➔ Für die Erarbeitung und Umsetzung von Informationssicherheitsmaßnahmen bedeutet dies, dass bereits zu Beginn gemeinsam klare Zielvorgaben erarbeitet und immer wieder überarbeitet werden müssen.

- Zusammensetzung des Projektteams evtl. sehr heterogen und ohne lange Zusammenarbeitserfahrung.

  ➔ Für die Erarbeitung und Umsetzung von Informationssicherheitsmaßnahmen bedeutet dies, dass möglichst bereits zu Beginn im Projektteam gleiche Voraussetzungen bspw. durch regelmäßigen Austausch geschaffen werden oder auch vorhandene Erfahrungen durch Weitergabe in den gemischten Projektteams genutzt werden.

Bei der Nichtberücksichtigung dieser Problemfelder können Zeitverzug, erhöhte Kosten und Aufwände oder eine fehlende oder unzureichende Umsetzung, d.h. ein fehlendes oder unvollständiges Ergebnis auftreten.

Bereits zu Projektbeginn sollten entsprechende Problemfelder des eigenen Projekts analysiert und berücksichtigt und individuelle Lösungen entwickelt werden. Hierzu muss bereits früh mit Risikomanagement hinsichtlich der Projektziele inkl. der Interessen aller Projektpartner, aber auch speziell in Bezug auf die Informationssicherheit im Gesamtprojekt begonnen werden.

Auch „Projektmanagement mit vielen Projektpartnern“ ist ein Themenkomplex aus dem PM. Hierbei ist ein gutes Stakeholder- und Erwartungsmanagement notwendig, um die unterschiedlichen Ziele aller Projektpartner zu berücksichtigen, um letztendlich alle Aspekte der Informationssicherheit erfolgreich bearbeiten zu können.

2. Ein weiteres wichtiges Thema ist die Klärung von Anforderungen im Bereich „Informationssicherheitsmanagement in vertraglichen Rahmenwerken“, die evtl. auch erst zur Laufzeit des Projekts entwickelt werden können. Siehe dazu auch das Ergebnisdokument zu AS 12.2.11 Maßnahmensammlung und Konsolidierung und das Lösungselement mit dem Titel „Umsetzung von Sicherheitsanforderungen bei Dritten“ aus dem enera Projektkompendium. Dort wird folgendes beschrieben:

> „Bei der Umsetzung von Sicherheitsanforderungen verhält es sich in der Praxis häufig so, dass nicht nur ein einziges Unternehmen allein dafür zuständig ist, vor allem dann, wenn Leistungen durch Dienstleister oder Partnerunternehmen erbracht werden, an welche die Gesamtverantwortung nicht vollständig abgegeben werden kann oder soll. In solchen Fällen müssen alle relevanten Sicherheitsanforderungen nicht nur vollständig identifiziert und umgesetzt werden, sondern diese Umsetzung muss in angemessener Weise vertraglich fixiert werden. Auf dieser Grundlage kann die Qualität und Vollständigkeit der Umsetzung bei Bedarf überprüft werden, z. B. zur Klärung von Fragen hinsichtlich Leistungserbringung und Haftung."

Es wird daher vorgeschlagen, sich die Wichtigkeit des Themenkomplexes Informationssicherheit bereits früh im Projekt bewusst zu machen und auftretende Probleme immer priorisiert zu behandeln. Dabei können Techniken aus dem Projektmanagement aber auch vertragliche Rahmenwerke verwendet werden. Auch Ergebnisse aus dem AS 12.2.13 zum Thema Security-by-Design (siehe auch Abschnitt 3.8 in diesem Dokument) können hierfür hilfreich sein.

3.7 Durchsetzen kontinuierlicher Informationssicherheit

Die Erkenntnis, dass Informationssicherheit nicht allein nur eine Produkteigenschaft ist, sondern ein Prozess, hat sich mittlerweile durchgesetzt. Zusätzlich wird auch das Security-by-Design-Prinzip3 immer relevanter und etabliert sich zunehmend. ISO / IEC definiert die notwendigen Arbeitsschritte dieses kontinuierlichen Prozesses, die man gut als PDCA-Zyklus4 darstellen kann, gemäß Abbildung 6.

[3] Siehe auch das Ergebnisdokument zu AS 12.2.13 „Anpassungen des Use Case-Templates hinsichtlich Security-by-Design".

[4] PDCA – Plan→DO→Check→Act: Der PDCA-Zyklus wird auch Deming-Kreis/-Zyklus genannt; er beschreib einen kontinuierlichen Verbesserungsprozess in vier Stufen.

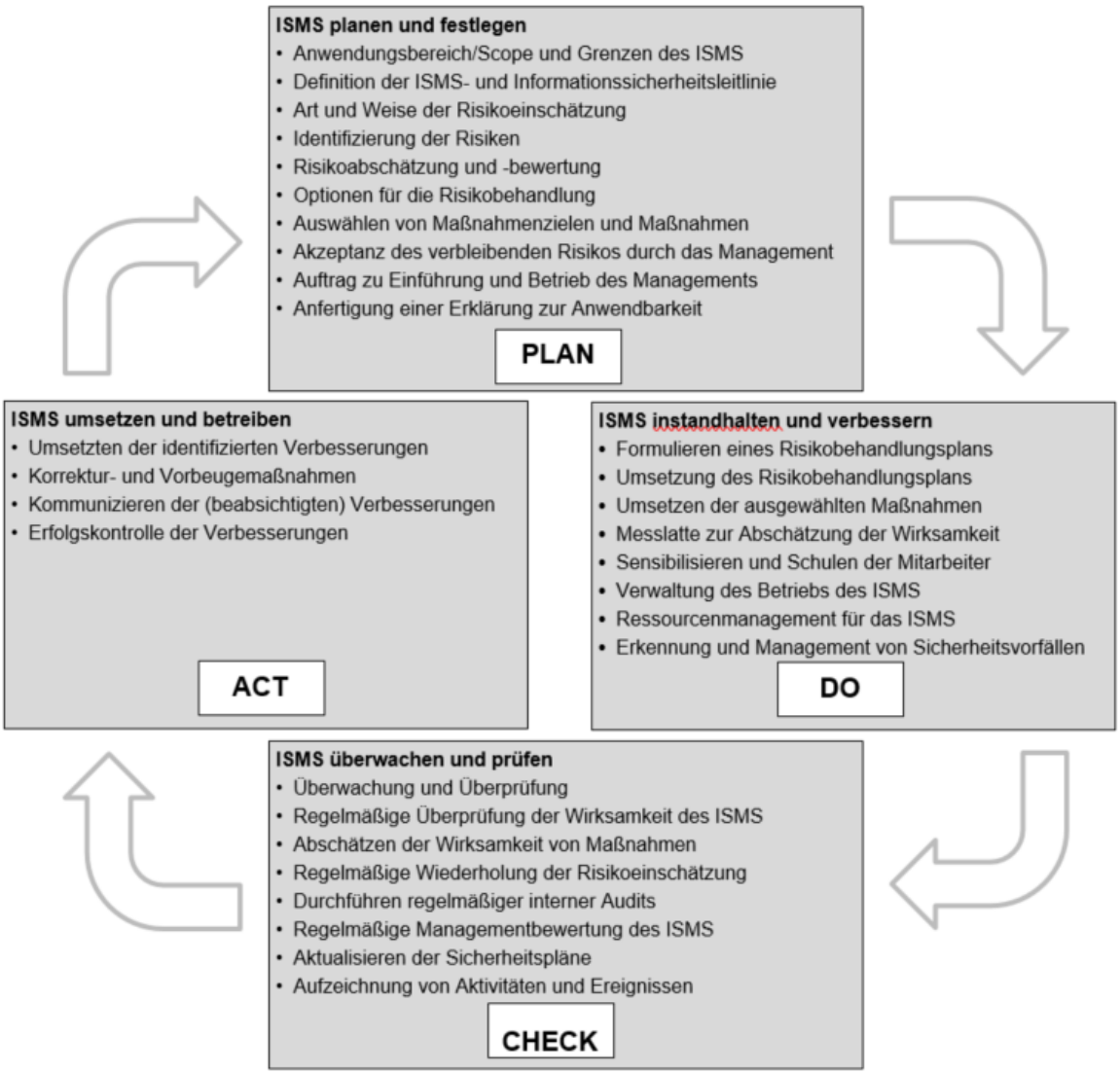


Abbildung 6: PDCA-Zyklus in der ISO/IEC 27001 [ENGEL 18]

Es ist allerdings schwierig, diesen Prozess auch kontinuierlich operativ umzusetzen, da oftmals die Dokumentation der Abläufe und Strukturen inkrementelle Veränderungen nicht gut unterstützt und bestimmte Analysen dann erneut gesamthaft durchgeführt werden müssen. Darüber hinaus werden zahlreiche Schritte für die Realisierung von Informationssicherheit erst im Nachgang der Umsetzung von IT-Projekten durchgeführt und nicht schon in der Planungsphase. Ziel sollte es sein, möglichst viele ISMS-Aufgaben schon in der Planungsphase durchzuführen, um die notwendige IT-Sicherheit schon in der Planungs- und Designphase festzulegen. Die Berücksichtigung von Informationssicherheit bei der Entwicklung sollte daher von den Schritten „Check“ und „Act“ in die Schritte „Plan“ und „Do“ vorgezogen werden, siehe Abbildung 7.

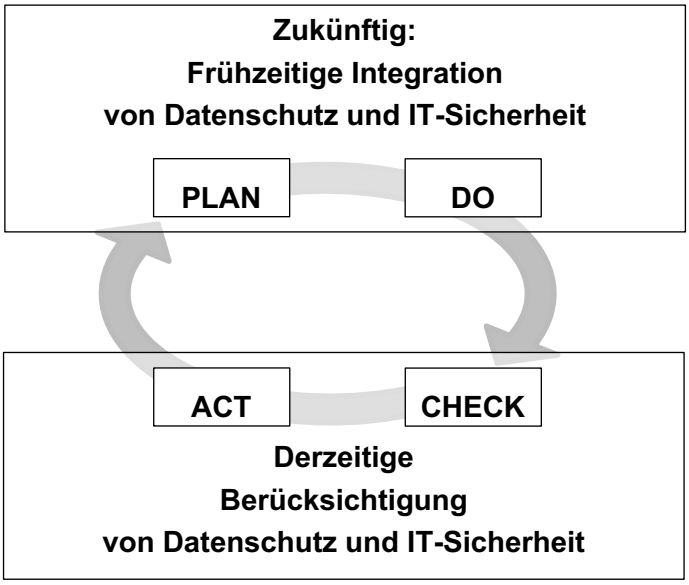


Abbildung 7: Transformation im PDCA-Zyklus komplexer Systeme [ENGEL 18]

Hier kann eine Dokumentation der geplanten und umgesetzten Abläufe und ggf. auch der Systemarchitektur auf Basis der IEC 62559 Use-Case-Methodik [IEC 15] hilfreich sein. So lassen sie die Anknüpfungspunkte zwischen neuen Abläufen oder Systemen und den schon bestehenden Systemen schnell ermitteln. Darüber hinaus fügt sich die neue Dokumentation medienbruchfrei in die bisherige Dokumentation ein.

3.8 Use-Case-Methodik nach IEC 62559 für Sicherheitsanalysen

Speziell bei einer werkzeugbasierten Verwaltung der Use Cases lassen sich Inkremente wie neue Datentypen, neue Systemkomponenten u. ä. schnell identifizieren und im Anschluss die entsprechenden zusätzlichen Schutzbedarfsfeststellungen für ebendiese treffen.

Allerdings bietet die Use-Case-Methodik nach IEC 62559 nur wenig Security- oder Safety-spezifische Unterstützung, um die besonderen Anforderungen im Sinne eines ISMS herauszuarbeiten und die Sicherheitszusammenhänge zu dokumentieren. Schutzbedarfe bezüglich funktionaler Sicherheit oder bezüglich Informationssicherheit können zwar als „Safety Considerations“ bzw. „Security Considerations“ an die Beschreibung der Transaktionsschritte angehängt werden. Darüber hinaus besteht auch noch die Möglichkeit, Sicherheitsziele als „Objectives“ eines Use Cases ausdrücklich zu spezifizieren; gegebenenfalls könnte man sie auch in Form einer geforderten Nachbedingung („Postcondition“) eines Anwendungsszenarios vermerken.

Im Grundsatz werden Sicherheitsaspekte in der Use-Case-Methodik nach IEC 62559 aber genauso wie alle übrigen nichtfunktionalen Anforderungen (z. B. Performanz, Benutzerfreundlichkeit, Wartbarkeit oder Skalierbarkeit) behandelt. Der Pre-Standard IEC/PAS 62559 [IEC/PAS 08] empfiehlt dazu lediglich, bei der Analyse der Use Cases stets auch die potentiellen Sicherheitsrisiken mitzubedenken und zu prüfen, welche System Assets bedroht sind und welche Verwundbarkeiten sie möglicherweise haben.

Die Anwendungsbeschreibung für das Use Case Template gemäß IEC/PAS 62559:2008 legt allerdings nicht fest, wie etwa Safety-Anforderungen oder notwendige Vorbedingungen systematisch bestimmt oder auf Stimmigkeit und Vollständigkeit untersucht werden können. Hierzu sind ergänzende Verfahren und Modelle erforderlich – welche, das bleibt dem Anwender überlassen.

Für eine noch umfassendere Unterstützung von Sicherheitsanalysen würde man sich über die im Template vorgesehenen Attribute hinaus noch weitere ausdrückliche Angaben wünschen, wie etwa:

- eine Auflistung der Sicherheitsannahmen: Vorbedingungen für eine sichere Durchführung des Anwendungsfalls
- eine Auflistung absehbarer Misuse-Cases zusammen mit den zugrundeliegenden Motiven für einen Misuse
- eine Erfassung möglicher Angreifer (Threat Agents) und ihrer charakteristischen Attribute (z. B. verfügbare Zeit- und Ressourcen, Skill Level, Angriffsmotive)
- auszuschließende Anti-Ziele: Was darf auf keinen Fall passieren?
- beteiligte Funktionsassets (Prozesse, Schnittstellen) und deren Schutzbedarf
- beteiligte physische Assets (Hardware) und deren Schutzbedarf

Angesichts des Umfangs des existierenden Use Case Templates und den Schwierigkeiten der Stakeholder, zu den geforderten Attributen sinnvolle Angaben zu machen, muss man jedoch sehr sorgfältig abwägen, welche der prinzipiell wünschenswerten Angaben tatsächlich Eingang in die Formatvorlage zur Anwendungsfallbeschreibung finden sollen.

Im Projekt enera wurde das von OFFIS bereitgestellte Use Case Management Repository (UCMR) mit dem ARIS-System der Software AG dergestalt verknüpft, dass die Erstellung und Pflege der Use Cases im UCMR und die Auswertung der Use-Case-Informationen für die Erstellung eines Sicherheitskonzepts in ARIS implementiert wurde. Damit besteht die Möglichkeit, bei zukünftigen Änderungen an den Use Cases und einem Reimport der Use-Case-Informationen in ARIS dort die Auswertung erneut zu starten.

Dabei ist die im Projekt enera entwickelte Lösung aber eher als ein Proof of Concept für die systemische Verknüpfung zu sehen. Die Ergebnisse machen aber Mut, dass eine entsprechende Erweiterung der Use-Case-Methodik hier einen deutlichen Mehrwert bringen kann. Somit wäre sowohl die Erfassung von Use Cases als auch die Durchführung der Sicherheitsanalyse innerhalb eines Managementtools wünschenswert. Ein entsprechendes New Working

Item Proposal (NWIP) über die Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE (DKE) und das IEC System Committee Smart Energy (IEC SyC SE) wäre empfehlenswert.

Laut Rolf Apel (Siemens, Convenor IEC SyC SE WG 5[5]) könnte man diesen Punkt in der Standardisierung einbringen, indem man die in enera erzielten Ergebnisse bei der DKE als NWIP (New Work Item Proposal) anbietet.

3.9 Erstellung von Informationsobjekt-Katalogen

Die Use-Case-Methodik gemäß IEC 62559 besteht in ihrem Kern aus der Dokumentation der zeitlichen Abfolge von Informationsflüssen zwischen den am Use Case beteiligten Aktoren. Analog zu den Aktoren bedarf es auch hier einer Use-Case-übergreifenden Vereinheitlichung der Terminologie, um auch die Informationsschnittstellen zwischen verschiedenen Use Cases richtig identifizieren zu können.

Idealerweise sollten daher Informationsobjekt-Kataloge der ausgetauschten Objekte erstellt werden, bevor mit der Erstellung der Use Cases begonnen wird. Speziell bei der werkzeugbasierten Use-Case-Erstellung werden auf diese Weise Terminologieprobleme bei der (semantischen) Benennung von Informationsobjekten vermieden.

Es ist allerdings sehr schwierig, im Vorhinein alle Datenflüsse und ausgetauschten Information zu überblicken, um einen umfassenden Informationsobjekt-Katalog aufzubauen. Da die meisten Schnittstellen für Informationsflüsse aber auf offenen internationalen Standards basieren, könnte hier über die (internationale) Standardisierung Abhilfe geschaffen werden. Viele internationale Kommunikationsstandards beinhalten mittlerweile auch eine Datenmodellbeschreibung für die übertragenen Informationen, wie z. B. die IEC 61850 oder die IEC 61968/70 (CIM). Die in diesen Standards verwendete Datenstruktur und Terminologie könnte als Basis für einen Informationsobjekt-Katalog verwendet werden. Allerdings sind die bestehenden Standards nicht überschneidungsfrei und es gibt oftmals, wie etwa bei den Standards IEC 61850 oder die IEC 61970, keine Abbildungsvorschriften für den überlappenden Bereich der Standardfamilien. Hier ist die Standardisierung gefordert, entsprechende Ontologien zu schaffen, um eine eineindeutige Abbildung zwischen Informationsobjekten mit gleicher Bedeutung und unterschiedlicher Terminologie zu ermöglichen.

Darüber hinaus sollten Informationsobjekt-Kataloge auch unterschiedliche Detailierungsebenen unterstützen und dabei auch die Zusammenhänge zwischen den verschiedenen Detailierungsstufen abbilden können. Im Projekt enera z. B. wurden für die Schutzbedarfsanalyse die

[5] Siehe auch https://www.iec.ch/dyn/www/f?p=103:14:9610819883655::::FSP_ORG_ID,FSP_LANG_ID:12610,25.

detaillierten Informationsobjekte aus den ausgewerteten Use Cases auf ein „High-Level-Datenmodell“ abgebildet[6], für dessen Ausprägungen dann die Schutzbedarfsfeststellung[7] erfolgte. Neben den Abbildungsvorschriften für gleichbedeutende Informationsobjektbezeichnungen zwischen Standards bedarf es der Einführung einer Art Hierarchie (Taxonomie), die angibt, ob es zu einem Informationsobjektbezeichner einen übergeordneten Sammelbegriff gibt. Beispiel: Die Informationsobjektbezeichnungen „Straßenname“, „Hausnummer“, „Postleitzahl“, „Stadt“, „Bundesland“ können unter dem Begriff „Adressdaten“ subsummiert werden. Solch eine Begriffshierarchie könnte von der Standardisierung im Rahmen eines durchgängigen Terminologiemanagements implementiert werden.

Weiterhin besteht die Möglichkeit, anhand der High-Level-Informationsobjekte bereits Vorschläge für die Schutzbedarfsfeststellung für die Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit oder auch in Bezug auf Datenschutz zu hinterlegen, so dass bei zukünftigen Sicherheitsanalysen ein schnelleres und vereinfachtes Vorgehen möglich ist.

Ende Februar 2019 hat CEN/CENELEC das Thema einer domänenübergreifenden Ontologie mit einem Workshop[8] aufgegriffen, um mit Experten darüber zu diskutieren, wie diese Aufgabenstellung angegangen werden kann. Weitere Schritte sind angekündigt und müssen abgewartet werden.

3.10 Goal Structuring Notation für ein nachvollziehbares Sicherheitsdesign

Gerade für Systeme wie einem Smart Grid, die einem ständigen Wandel unterliegen, ist ein kontinuierliches Sicherheitsmanagement eine Herausforderung. Wie in den Abschnitten 3.7 und 3.8 dargestellt, kann die Aufrechterhaltung von Sicherheitsanforderungen durch eine sorgfältige Use-Case-Modellierung unterstützt werden. Allerdings dokumentiert der Use Case vornehmlich die *Ergebnisse* einer Schutzbedarfsfeststellung; wie dieser Befund zustande kam ist hingegen nicht immer so ohne Weiteres nachvollziehbar.

Um auch bei beständigen Änderungen und Erweiterungen eines Energienetzes den Überblick zu behalten, ob alle maßgeblichen Sicherheitsziele noch erreicht werden, muss die Argumentation, warum das System als sicher gelten darf, nachvollziehbar und jederzeit überprüfbar sein. Hier bietet die Goal Structuring Notation (GSN) [SCSC 18] eine Möglichkeit, Sicherheits-

[6] Das High-Level-Datenmodell ist in der enera owncloud unter /Enera/AP12/AS 12.2.07 - Strukturanalyse und Inventarisierung/HL-Infoobjekte etc abgelegt.

[7] Siehe auch das Ergebnisdokument zur Schutzbedarfsfeststellung aus AS 12.2.8. Informationen zum HL-Datenmodell werden dort in Kapitel 4 beschrieben.

[8] Informationen zum “Workshop on Mapping Ontologies“, siehe https://www.cencenelec.eu/news/articles/Pages/AR-2018-045.aspx.

ziele, Annahmen, Begründungsstrategien, Begründungen und technische Sicherheitslösungen zueinander in Beziehung zu setzen. Damit wird nachvollziehbar, wo einzelne Sicherheitsanforderungen (sowohl bezüglich Security als auch bezüglich Safety) herrühren und wie sie in ihrem Zusammenspiel gewährleisten, dass ein übergeordnetes Sicherheitsziel auch tatsächlich erreicht wird. Ändert sich das System, so kann die in GSN modellierte Argumentationskette erneut durchlaufen werden, um zu prüfen, ob alle Annahmen und Schlussfolgerungen noch stimmig sind und ob die zur Lösung des Sicherheitsproblems vorgesehenen Lösungsbausteine zusammen noch immer zum vorgegebene Ziel führen. Ergeben sich durch Systemänderungen Lücken in der zugrundeliegenden Sicherheitsstrategie, so werden diese anhand des GSN-Modells leichter augenfällig als in einer ergebnisorientierten Anforderungs- oder Use-Case-Spezifikation.

Im Rahmen des Projekts enera wurde anhand eines Fallbeispiels dargestellt, wie sich grundlegende funktionale Sicherheitsziele oder auch IT-Sicherheitsziele mittels GSN Schritt für Schritt in hierarchisch strukturierte Unterziele verfeinern lassen, bis sie schließlich auf unmittelbar nachvollziehbare Lösungsbausteine reduziert sind. Entlang dieser Verfeinerungshierarchie kann sowohl die Argumentationsstrategie und deren Rechtfertigung, als auch die dabei getroffenen Annahmen in entsprechenden Annotationen festgehalten werden; außerdem kann der genauere Kontext und dessen Einschränkungen beschrieben werden, in dem diese Argumentationskette gelten soll. Bei Systemänderungen sind diese Argumente damit einer Überprüfung zugänglich. Dadurch wird Sicherheit besser wartbar.

Tabelle 2 zeigt, wie sich das Use-Case-Modell mittels GSN anreichern lässt, um eine Schutzbedarfsfeststellung nachvollziehbarer zu begründen und sie wartbarer zu gestalten. Einschlägige Smart-Grid-Standards berücksichtigen GSN derzeit allerdings nicht als Modellierungsansatz.

GSN-Element	Use Case Element	Abweichung
Goal	1.3 Objective	Objective-ID zur einfachen Referenzierung fehlt.
Strategy	—	Ein schlüssiger Zusammenhang zwischen einem Ziel und seinen Teilzielen bzw. Requirements ist derzeit nicht dokumentiert.
Solution	6 Requirement	
Context	1.3 Scope	Der Kontext ist nur für den gesamten Use Case dokumentiert und nicht spezifisch für Teilziele oder Strategien.
Assumption	1.6 Assumptions	Annahmen können dokumentiert werden, jedoch nur ohne Verweis auf andere Elemente.
Justification	—	Möglichkeit, explizit eine Begründung für ein Ziel oder eine Strategie zu hinterlegen, fehlt
SupportedBy	Verweis auf Element mit ID	Derzeit nur Verweise auf Elemente mit einer ID möglich.

GSN-Element	Use Case Element	Abweichung
		Keine durchgängige Kette von Ziel bis Requirement vorgesehen.
InContextOf	—	Verweise auf Kontext, Annahme und Begründung derzeit nicht vorgesehen.

Tabelle 2: Zuordnungsmatrix GSN zu UCMR-Modellelementen aus [IESE 19]

3.11 Grundschutzprofil z. B für Smart Home

Im Kontext von AP12 hat sich herausgestellt, dass es sinnvoll ist, Vorlagen für ISMS bzw. für Komponenten eines ISMS z. B. in Form eines sog. IT-Grundschutzprofils vorliegen zu haben, um vorhandene Erfahrungen und Bewertungen für eine ausreichende Absicherung nutzen zu können. Im Lösungselement des enera Projektkompendiums mit dem Titel „ISMS-Scope: „Messen und Steuern via SMGW“ – Schritte zur Einführung eines Informationssicherheitsmanagementsystems nach BSI IT-Grundschutz“ wurde in Bezug auf das Smart Home bereits folgendes beschrieben: „Die Umsetzung von vorgeschlagenen Sicherheitsmaßnahmen in privaten Anlagen, Wohn- und sonstigen Gebäuden liegt vielfach nicht im Einflussbereich eines SMGW-Administrators, MSB oder EMT. Daher thematisieren die Vorschläge aus enera vor allem eine Erhöhung des Risikobewusstseins bei den Betreibern der CLS, sowohl unter Aspekten des Datenschutzes als auch hinsichtlich finanzieller Auswirkungen bei Ausfällen unterschiedlicher Ursache.“.

Es wird daher empfohlen, IT-Grundschutzprofile oder andere Vorlagen / Blaupausen für die Erstellung eines ISMS für das Smart Home zu entwickeln. Weiterhin kann es helfen, dies ebenfalls für bestimmte Domänen oder einen Bereich in einer Domäne zu erarbeiten und zur freien Verfügung zu stellen. Dies hilft bspw. kleinen und mittelständischen Unternehmen dabei, eine bessere Absicherung ihrer Informationsinfrastruktur zu erreichen. Kontinuierlich und systematisch angewendet kann dies sogar Deutschlandweit, in der EU, bis weltweit zu einer besser abgesichert Informations- und Kommunikationstechnik führen.

4 Zusammenfassung und Ausblick

Dieses Ergebnisdokument hat im Rahmen von enera in AP12 elf verschiedene Lücken für den Themenbereich Informationssicherheit in der Energiedomäne, häufig im Zusammenhang mit Standardisierung und Normung, identifiziert, aufgezeigt und, wenn möglich, potenzielle Lösungen präsentiert. Die Lücken und deren mögliche Lösungen sind in der folgenden Tabelle nochmal kurz zusammengefasst.

Abschnitt-Nr.	Relevante Lücken	Mögliche Lösungen
3.1	Methodik nach NIST IR 7628 erweitern	Methoden der Richtlinie VDE 0175-110 im europäischen Kontext verwenden und durch weitere relevante Standards erweitern.
3.2	Lücken in Regularien aus AS 12.2.1	Diese Lücken wurden in AS 12.2.4 bearbeitet.
3.3	Zertifizierung eines ISMS: Nach IT-Grundschutz ermöglichen	Zertifizierung von Energieversorgern nach IT-Sicherheitskatalog für ISMS auch gemäß ISO 27001 auf Basis von BSI IT-Grundschutz zulassen.
3.4	Zusammenführung Notfallmanagement	Notfallmanagement in Energieversorgungssystemen sollte auch fortschreitende Energiewende und Digitalisierung berücksichtigen.
3.5	Informationssicherheit versus Funktionssicherheit	Bei sicherheitstechnischer Konzeption der IT-Systeme in der Energieversorgung muss saubere Trennung der beiden Welten mit definierten Schnittstellen erfolgen.
3.6	Informationssicherheitsmanagement bei vielen Partnern	Anforderungen zum Informationssicherheitsmanagement (frühzeitig) berücksichtigen. Managementtechniken und vertragliche Rahmenwerke verwenden.
3.7	Durchsetzen kontinuierlicher Informationssicherheit	Kontinuierlichen Prozess für Informationssicherheit z. B. nach PDCA-Zyklus ist notwendig. ISMS-Aufgaben bereits in Planungsphase verlagern.
3.8	Use-Case-Methodik nach IEC 62559 für Sicherheitsanalysen	UC-Methodik in der Planungsphase für die systematische Einführung eines ISMS verwenden. Erweiterungen für ISMS im UC-Template, die in AP12 erarbeitet wurden, verwenden.
3.9	Erstellung von Informationsobjekt-Katalogen	Vereinheitlichung der Terminologie für Informationsobjekte idealerweise zu Beginn der Planungsphase. Integration von Vorschlägen für die Schutzbedarfsfeststellung der Informationsobjekte bspw. für CIA.

Abschnitt-Nr.	Relevante Lücken	Mögliche Lösungen
3.10	Goal Structuring Notation für ein nachvollziehbares Sicherheitsdesign	UC-Methodik durch GSN-Notation für die systematische Anforderungserfassung anreichern.
3.11	Grundschutzprofil z. B für Smart Home	Grundschutzprofil oder andere Vorlagen / Blaupausen für die Erstellung eines ISMS erarbeiten und zur freien Verfügung stellen.

Tabelle 3: Zusammenfassung relevanten Lücken mit möglichen Lücken

Die identifizierten Lücken mit möglichen Lösungen wurden durch die Projektpartner aus AP12 gesammelt und erarbeitet. Dieses Ergebnisdokument ist öffentlich einsehbar, die Inhalte werden durch die Projektpartner verteilt und proaktiv vertreten. Teilweise werden einzelne Ideen und Lösungen Eingang in verschiedene Gremien der Normung und Standardisierung finden.

Literaturverzeichnis

[BNA 20] Bundesnetzagentur (2020): IT-Sicherheitskatalog für den Energiesektor, URL: www.bundesnetzagentur.de/DE/Sachgebiete/ElektrizitaetundGas/Unternehmen_Institutionen/Versorgungssicherheit/IT_Sicherheit/IT_Sicherheit_node.html (Stand 19.05.2020).

[BSI 2020] Bundesamt für Sicherheit in der Informationistechnik: IT-Grundschutz-Kompendium 2020 im Internet, URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/IT_Grundschutz_Kompendium_Edition2020.pdf

IT-Grundschutz-Kompendium allgemein: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/it-grundschutz-kompendium_node.html

[ENGEL 18] Lukas Engel (2018): Entwicklung eines Transformationsansatzes zur Integration von Datenschutz und IT-Sicherheit in die Planungsphase komplexer Systeme; Masterarbeit MA0757-18 an der Professur für Qualitätswissenschaft im Lehrstuhl für Fertigungsmesstechnik an der Friedrich-Alexander-Universität Erlangen-Nürnberg.

[GABL 18] Gabler Wirtschaftslexikon (2018): Gap-Analyse. Online im Internet, URL: https://wirtschaftslexikon.gabler.de/definition/gap-analyse-34738 (Stand 25.03.2021).

[IEC 15] International Electrotechnical Commission (2015): IEC 62559-2:2015 Use case methodology – Part 2: Definition of the templates for use cases, actor list and requirements list. Hrsg.: IEC.

[IEC/PAS 08] International Electrotechnical Commission (2008): IEC/PAS 62559:2008 IntelligGrid Methodology for Developing Requirements for Energy Systems (Edition 1.0), Publicly Available Specification Pre-Standard. Hrsg.: IEC.

[IESE 19] Denis Uecker, Rasmus Adler, Reinhard Schwarz (2019): Gap-Analyse der Metamodelle des OFFIS Use Case Templates und der Goal Structuring Notation (Version 1.1). IESE Report, Fraunhofer IESE, Kaiserslautern.

[SCSC 18] Safety-Critical Systems Club Assurance Case Working Group (2018): Goal Structuring Notation Community Standard Version 2, York.

Abbildungsverzeichnis

Abbildung 1: Darstellung Gap-Analyse [GABL 18] 8
Abbildung 2: Sicherheitsanalyse-Methodik für Smart-Grids basierend auf NIST IR 7628 11
Abbildung 3: Vergleich der Priorisierung von Schutzzielen 14
Abbildung 4: Überblick Analyse und Ansatz für Implementierung 15
Abbildung 5: Empfohlene Struktur für Network Code bei Cybersicherheit 15
Abbildung 6: PDCA-Zyklus in der ISO/IEC 27001 [ENGEL 18] 19
Abbildung 7: Transformation im PDCA-Zyklus komplexer Systeme [ENGEL 18] 20

Tabellenverzeichnis

Tabelle 1: Statustabelle identifizierte Lücken (wurde regelmäßig aktualisiert) 10
Tabelle 2: Zuordnungsmatrix GSN zu UCMR-Modellelementen aus [IESE 19] 25
Tabelle 3: Zusammenfassung relevanten Lücken mit möglichen Lücken 27