RISIKOANALYSE FÜR DIE INFORMATIONSSYSTEME DER ELEKTRIZITÄTSWIRTSCHAFT

unter besonderer Berücksichtigung von Smart-Metern und des Datenschutzes

Veröffentlicht am 27.02.2014

Vorwort

Im Frühjahr 2012 wurde durch das Bundeskanzleramt (BKA) gemeinsam mit Expertinnen und Experten aus Wirtschaft, Wissenschaft und öffentlicher Verwaltung eine IKT (**I**nformations- und **K**ommunikations**t**echnologie)-Sicherheitsstrategie entwickelt. Diese Strategie hat als Kernziel den Schutz kritischer Informationsinfrastrukturen und fordert davon ausgehend die Umsetzung von Maßnahmen, die die Kalkulierbarkeit von Risiken sicherstellen. Referenziert man auf den 2012 erschienenen Bericht Cybercrime des BM.I, so ist die Cyberkriminalität in Österreich erheblich angestiegen. Auch CERT.AT weist im November 2013 erschienen Jahresbericht auf die Zunahme bei der Cyberkriminalität hin.

Die Abhängigkeit unserer Gesellschaft von der kritischen Infrastruktur Strom rückte in den letzten Monaten durch die Einführung der „Smart-Meter“ in den Fokus der öffentlichen Wahrnehmung. Die Diskussion rund um die IMA-VO, die die Anforderungen an intelligente Messgeräte konkretisiert, wurde z.T. sehr emotional und wenig faktenbasiert geführt.

Nicht zuletzt durch die Konvergenz mehrerer Sicherheitsstrategien in Österreich, die Österreichische Sicherheitsstrategie, die ÖSCS (Österreichische Strategie für Cyber Sicherheit) und dem APCIP-Programm (Österreichisches Programm zum Schutz kritischer Infrastrukturen), wurde auf Initiative der zwei Sicherheitsministerien BM.I und BMLVS sowie dem BMFWJ, dem Bundeskanzleramt, der Regulierungsbehörde und maßgeblichen Vertretern der Branche ein konsensualer Analyse- und Bewertungsprozess durchgeführt, der die Risiken für die Versorgungssicherheit mit Strom in Österreich durch die Nutzung von IKT-Infrastrukturen detailliert beleuchtet.

Dies stellt einen ersten Schritt zur Umsetzung vorgeschlagener Maßnahmen (z.B. Risikoanalyse bei Betreibern kritischer Infrastrukturen) in den aus den o.a. Strategien zur Erhöhung der Resilienz der Energiewirtschaft gegenüber IKT-Attacken und IKT-Gebrechen und -Fehler bei Stromerzeugern und Netzbetreibern dar.

Die genutzte IKT, auch die für den Einsatz von intelligenten Messgeräten (Smart-Meter), ist grundsätzlich verwundbar und angreifbar. Aufgrund der gestiegenen Vernetzung ist auch die Gefahr, Ziel krimineller Attacken zu werden, gestiegen. Damit sind per se auch Aspekte des Datenschutzes berührt, die einer Objektivierung des Risikoprofils bedürfen. Da es bis dato bundesweit keinen holistisch geprägten Gefahrenidentifikations- und Bewertungsprozess für die Energiewirtschaft aus dem Blickwinkel der Versorgungssicherheit und Nutzung moderner IKT gab, konnten auch die Risiken, die sich aus der Nutzung ableiten, nicht quantifiziert werden. IKT ist geprägt durch einen sehr hohen Innovationszyklus. Es bedarf daher neuer Sicherheitsarchitekturen, die zeitlich angepasst den identifizierten Risiken gegenüber gestellt werden müssen. Darum wurde diese Risikoanalyse als erster Schritt im Herbst 2012 initiiert und 2013 auf einer breiten Wissensbasis konsensual durchgeführt.

Kurzfassung

Die vorliegende Risikoanalyse ist das Ergebnis einer gemeinsamen, auf freiwilliger Basis stattgefundenen Kooperation zwischen dem österreichischen Bundeskanzleramt, sicherheitsrelevanter Ministerien, Branchenvertretern der österreichischen Energiewirtschaft und der Energie-Control Austria als zuständiger Regulierungsbehörde. Auslöser war die zum Teil emotional geführte Diskussion um Sicherheitsaspekte rund um die bevorstehende Einführung der Smart-Meter Technologie. Fokus der Analyse war die Betrachtung der zur Sicherstellung der Versorgungssicherheit systemrelevanten IKT-Systeme und –Bereiche der Energiewirtschaft.

Daher wurden nur Risiken, die potentiell einen nennenswerten, flächendeckenden Stromausfall verursachen können, identifiziert, kommerzielle Gefahren wurden von der Betrachtung ausgeschlossen.

Die Projektstruktur bestand aus einem Lenkungsausschuss und aus einem technischen Expertengremium. Insgesamt wurden zur Erstellung dieser Analyse neun Workshops durchgeführt, wobei ab dem dritten Workshop eine erweiterte Expertengruppe im Rahmen der Mitglieder von „Oesterreichs Energie“ mit einbezogen wurde. Vertreter aus den beiden Sicherheitsressorts BM.I und BMLVS sowie dem BKA standen der Risikoanalyse unterstützend zur Seite. Zusätzlich war das BMWFJ mit eingebunden.

Das Projekt ist damit ein Vorzeigemodell für eine gelebte Public-Private-Partnership (PPP). In einem Beispiel gebenden Verfahren wurden durch Vereinbarung eines „Traffic-Light“-Protokolls vertrauliche Informationen bedarfsgerecht zur Verfügung gestellt. Die gesamte Kommunikation zwischen den Vertretern des Expertengremiums wurde verschlüsselt durchgeführt, um gelebte Sicherheit in einem PPP-Modell zu praktizieren. Dies trug insgesamt zu einer vertrauensvollen und überaus konstruktiven Zusammenarbeit bei.

Parallel zu den Expertenworkshops wurden 28 Expertengespräche mit Vertretern der Wirtschaft und der Wissenschaft geführt.

Die Risikoanalyse gliedert sich in vier Teile. Der erste Teil liefert eine Beschreibung der allgemeinen Herangehensweise und Methode zur Risikoidentifikation und Bewertung.

Teil II stellt den internen und den externen Kontext entsprechend ISO 31.000:2010 her und beschreibt die Rahmenbedingungen für die Risikoanalyse.

Teil III stellt die Ergebnisse der Gefahrenidentifikation und Bewertung der Risiken dar und leitet daraus Maßnahmen zur Risikominimierung und –Bewältigung ab.

Teil IV beschreibt die aus den abgeleiteten Maßnahmen resultierenden Empfehlungen.

Im Zuge der Arbeiten an Teil III wurden insgesamt 15 Gefahrenfelder identifiziert, aus denen wiederum 114 Einzelgefahren zusammengestellt und analysiert wurden.

Die Bewertung dieser 114 Einzelgefahren führte zur Identifikation von 73 Einzelrisiken, die in weiterer Folge zu 19 Aggregationsrisiken verdichtet wurden.

Als Grundlage für die Risikoanalyse und Erarbeitung von Maßnahmen wurde der „Worst-Case“-Fall herangezogen.

Die Risikoanalyse wurde mit der Abnahme des vorliegenden Berichts durch den Lenkungsausschuss abgeschlossen.

Inhaltsverzeichnis

Verzeichnis der Abbildungen

Verzeichnis der Tabellen

Teil I Allgemeines

1 Aufbau der Risikoanalyse

Die vorliegende Risikoanalyse liegt in vier Teilen vor.

Teil I beschreibt die allgemeine Herangehensweise und Methode zur Risikoidentifikation und Bewertung. Die Vorgehensweise orientiert sich an den Vorgaben der ISO 31.000:2010 Risk management, der ONR 49.002-2:2010, Risikomanagement für Organisationen und Systeme, Leitfaden für die Methoden der Risikobeurteilung sowie der ÖNORM S 2410:2010 Chancen- und Risikomanagement. Im ersten Teil wird auch die „Wissensbasis“ sowie die spezifische Literaturzusammenstellung aufbereitet. Diese Zusammenstellung kann bei Bedarf 1:1 in ein Intranet übernommen werden.

Im Teil II wird der interne und externe Kontext gemäß ISO 31.000:2010 hergestellt. Im Wesentlichen handelt es sich dabei um eine kurze Beschreibung der Rahmenbedingungen für die Risikoanalyse und, abgeleitet von der Österreichischen Sicherheitsstrategie, relevante Zusammenhänge zur Österreichischen Strategie für Cybersicherheit ÖSCS.

Der Teil III stellt die Ergebnisse der Gefahrenidentifikation und Bewertung zu Risiken dar.

Hier wird im ersten Schritt das Werkzeug für die Gefahrenidentifikation dargestellt. Dazu wurden alle relevanten Kommunikationsbeziehungen, die einen Bezug zur Nutzung von IKT-Infrastrukturen darstellen, zusammengestellt. Aus diesen Kommunikationsbeziehungen erwachsen denkbare Gefahren, die es zu identifizieren gilt. Aufbauend auf diesen Arbeiten werden Einzelgefahren zu Einzelrisiken bewertet und anschließend zu Aggregationsrisiken zusammengefasst. Der letzte Ergebnisschritt ist die Ableitung von Maßnahmen zur Minimierung und Bewältigung von erkannten Risiken.

Aus den abgeleiteten Maßnahmen werden im Teil IV Empfehlungen ausgesprochen.

An dieser Stelle sei darauf hingewiesen, dass eine Risikoanalyse lediglich eine Teilaufgabe eines kontinuierlichen Verbesserungsprozesses darstellt. Um fortfolgende Arbeiten optimal zu unterstützen, wurden daher alle Zwischenergebnisse und Ergebnisse in den Anhängen zusammengestellt und aufbereitet. Die Datengrundlagen und erarbeiteten Risikomatrizen liegen auf einer CD-R so aufbereitet bei, dass diese bei Bedarf in ein Intranet übernommen werden bzw. auf elektronischem Weg ausgetauscht werden können.

2 Zielsetzungen und Hintergrund der Risikoanalyse

2.1 Allgemeine Zielsetzungen der Risikoanalyse

Das Ziel der vorliegenden Risikoanalyse ist es, Gefahren zu identifizieren, die einen **nennenswerten** und **flächendeckenden** Stromausfall durch:

- die Nutzung und Anwendung von Informations- und Kommunikationstechnologie
- Natur- und Elementarereignisse
- kriminelle und/oder terroristische Aktivitäten (Intentionale Gefahren) im Cyberraum bzw. mit den Mitteln der Informations- und Kommunikationstechnologie

hervorrufen können. Insbesondere bei „Intentionalen Gefahren“ werden Belange des Datenschutzes mit angesprochen.

Eine bindende Festlegung bzw. eine Definition für einen nennenswerten Stromausfall in Österreich gibt es bis dato nicht. In Deutschland wurde ein „worst-case“ Szenario in der Bundestagsdrucksache 17/5672 definiert. Darin wird ein „black-out“ Szenario für die Dauer von 8-10 Tagen skizziert.[1] Die Rahmenbedingungen für die Festlegung eines für Österreich flächendeckenden und nennenswerten Stromausfalls werden im Kapitel 9 definiert.

Das übergeordnete Ziel der Risikoanalyse ist es daher, Risiken im Kontext des Einsatzes von IKT-Infrastrukturen zu erfassen und mit Blick auf die Versorgungssicherheit in Österreich zu bewerten.

Der Terminus „IKT-Infrastruktur“ wird im Umfeld von Netzbetreibern bzw. EVUs als Sammelbegriff von:

- zentralisierten Systemen, die der Prozesssteuerung und –überwachung sowie der der Betriebsführung im Bereich Prozesssteuerung dienen,
- Prozesstechnik, die zur Sprach- und Datenkommunikation Übertragungs-, Telekommunikations- und Netzwerktechnik verwendet, verstanden
- prozessnaher Steuerungs- und Automatisierungstechnik mit zugehörigen Schutz- und Safety-Sytemen und fernwirktechnischen Komponenten definiert.

Eine historisch belegte Abgrenzung in klassische „Primär-, Sekundär, Fernwirk- und Netzleittechnik“ wird immer schwieriger, da der immer stärker werdende Standardisierungsdruck eine Assemblierung von COTS-Produkten zu „funktionalen Einheiten“ eine historisch bedingte Abgrenzung von „elektronischen und elektrischen Komponenten“ ad absurdum führt.

[1] Siehe Lit. ECA-13, Bundestagsdrucksache, die auf einen Bericht des Büros für Technikfolgen-Abschätzung beim Deutschen Bundestag basiert, Seite 32, Kapitel 2 Folgen für Kritische Infrastrukturen in Deutschland

2.2 Nichtziele der Risikoanalyse

Die österreichische Elektrizitätswirtschaft gilt als sehr stabil mit hoher Verfügbarkeit. Die durchschnittliche Nichtverfügbarkeit (alle, geplante und ungeplante) in Österreich (ASIDI) im Jahr 2012 betrug 54[2] min.

Die Wirkdimension für die Risikoanalyse sind ausschließlich nennenswerte Stromausfälle, die durch Störungen, Fehler oder absichtliche Manipulationen an der IKT-Infrastruktur bedingt sind. Monetäre Schäden für den Netzbetreiber, Erzeuger oder für den Stromhandel werden nicht bzw. nur indirekt betrachtet. Im Rahmen der Arbeiten zur Risikoanalyse wurden auch die Ergebnisse aus dem KIRAS Projekt „Blackout Ö1“ verwertet. Um die Risikoanalyse insgesamt auch aus der wirtschaftlichen Sicht einzuordnen, wird hier ein exemplarischer Überblick über mögliche volkswirtschaftliche Schäden durch einen Stromausfall in Österreich gegeben.

2.2.1 Volkswirtschaftliche Schäden durch einen flächendeckenden Stromausfall

Um die volkswirtschaftlichen Schäden eines nennenswerten Stromausfalls herauszuarbeiten, wurde eine exemplarische Auswertung der Johannes Kepler Universität Linz mit dem Modell „Apostel“[3] durchgeführt.

In der Annahme, der Stromausfall würde am 16.01.2013 stattfinden, hätte um 08:00 begonnen und wäre nach 5 Stunden wieder beendet, ergäben sich für Österreich, getrennt dargestellt nach Bundesländern, folgende volkswirtschaftliche Auswirkungen:

Dauer	Wien		Niederösterreich		Burgenland	
	1.000 €	MWh	1.000 €	MWh	1.000 €	MWh
3 Stunden	92.358	2.781	42.749	3.510	4.631	354
5 Stunden	122.159	4.635	56.987	5.849	6.042	590
10 Stunden	171.392	9.271	80.961	11.699	8.459	1.181
24 Stunden	283.480	22.250	133.433	28.077	13.293	2.834
48 Stunden	501.210	44.500	237.338	56.154	23.991	5.668

Tabelle 1: Volkswirtschaftliche Schäden eines Stromausfalls (Teil 1)

Interpretation: Ein 5-stündiger Stromausfall, der exakt innerhalb der politischen Grenzen des Bundeslandes Wien stattfindet und am 16.01.2013 um 8 Uhr morgens beginnt, verursacht 122 Mio. € volkswirtschaftlichen Schaden, und 4.635 MWh elektrische Energie können während dieser Zeit nicht zu den Endkunden transportiert werden.

[2] Siehe Lit. ECA-16, Österreichische Ausfalls- und Störstatistik der E-Control

[3] Siehe Lit. ECA-60, Apostel, Johannes Kepler Universität, übermittelt von Dr. Reichl, 16.04.13

Dauer	Steiermark		Oberösterreich		Kärnten	
	1.000 €	MWh	1.000 €	MWh	1.000 €	MWh
3 Stunden	28.944	3.077	45.557	4.851	13.466	1.478
5 Stunden	38.153	5.128	60.307	8.085	17.740	2.463
10 Stunden	54.032	10.256	84.985	16.169	25.040	4.926
24 Stunden	86.588	24.614	138.323	38.807	40.185	11.823
48 Stunden	156.452	49.228	244.718	77.613	72.020	23.646

Tabelle 2: Volkswirtschaftliche Schäden eines Stromausfalls (Teil 2)

Dauer	Tirol		Vorarlberg		Salzburg	
	1.000 €	MWh	1.000 €	MWh	1.000 €	MWh
3 Stunden	19.252	1.870	11.599	1.617	21.784	1.326
5 Stunden	25.145	3.116	15.177	2.696	28.999	2.211
10 Stunden	35.354	6.233	21.098	5.391	40.802	4.421
24 Stunden	55.469	14.958	33.745	12.939	67.794	10.611
48 Stunden	100.268	29.917	59.563	25.877	118.378	21.222

Tabelle 3: Volkswirtschaftliche Schäden eines Stromausfalls (Teil 3)

Die in dem vorgestellten Modell definierten Randbedingungen und Annahmen waren u.a. auch die konzeptionellen Grundlagen, um die Bewertungskriterien (vgl. dazu auch Kapitel 9) für einen flächendeckenden, nennenswerten Stromausfall in Österreich zu definieren.

2.3 Allgemeine Rahmenbedingungen der Risikoanalyse

Im Rahmen der Risikobewertungen müssen Aussagen zu „Erwartungswerten“ für Stör- oder Schadereignisse prognostiziert oder besser abgeschätzt werden.

Der Prognosehorizont für die Erfassung und Bewertung der Risiken wurde bis 2020 festgelegt.

In vielen Fällen, insbesondere bei der Bewertung von intentionalen Gefahren, verfügt man bis dato über wenig Erfahrung bzw. belastbare Daten, um eine objektivierte „Prognose“ zu Eintrittswahrscheinlichkeiten abgeben zu können.

Um für alle drei Gefahrenfelder, technische Gefahren, Naturgefahren und intentionale Gefahren, gemäß ÖNORM S2401[4] eine einheitliche Risikomatrix abbilden zu können, wurden die Bewertungskriterien für die Eintrittswahrscheinlichkeiten für technische Gefahren und Naturgefahren zusammengefasst. Parallel dazu wurde die Eintrittswahrscheinlichkeit für intentionale Gefahren nur implizit über abgeschätzte Häufigkeiten pro Zeiteinheit von möglichen „Ereignissen, Attacken und Penetrationen“, sondern vielmehr über den Begriff der Machbarkeit hergeleitet und diese in Relation zueinander gesetzt.

[4] Siehe Lit.ECA-61, ÖNORM S2401, Business Continuity und Corporate Security Management, “Systemaufbau und Business Continuity und Corporate Security Policy”

Es wird daher darauf hingewiesen, dass die identifizierten und bewerteten Risiken immer nur **in Relation zueinander** eine valide Aussage erlauben, da nicht der Anspruch erhoben wird, dass die identifizierten Risiken eine *absolute* Position in der Risikomatrix einnehmen.

3 Methodik der Risikoanalyse

Die Risikoanalyse wurde gemäß den Rahmenvorgaben der ISO 31.000 bzw. der ONR 49.002-1:2010 durchgeführt. Dazu wurden seitens der Projektleitung drei maßgebliche Projekt- und Arbeitsgruppen eingerichtet.

1. Lenkungsausschuss, der die Schnittstelle zur ÖSCS, zur Österreichischen Sicherheitsstrategie, zu EPCIP und zum APCIP-Programm darstellt
2. Projekt-Kernteam, bestehend aus Vertretern der Wirtschaft und der Ministerien sowie CERT.AT
3. Erweitertes Projektteam aus Experten der E-Wirtschaft

Der Risikoerfassungs- und -bewertungsprozess wurde gemäß Abbildung 1 durchgeführt.

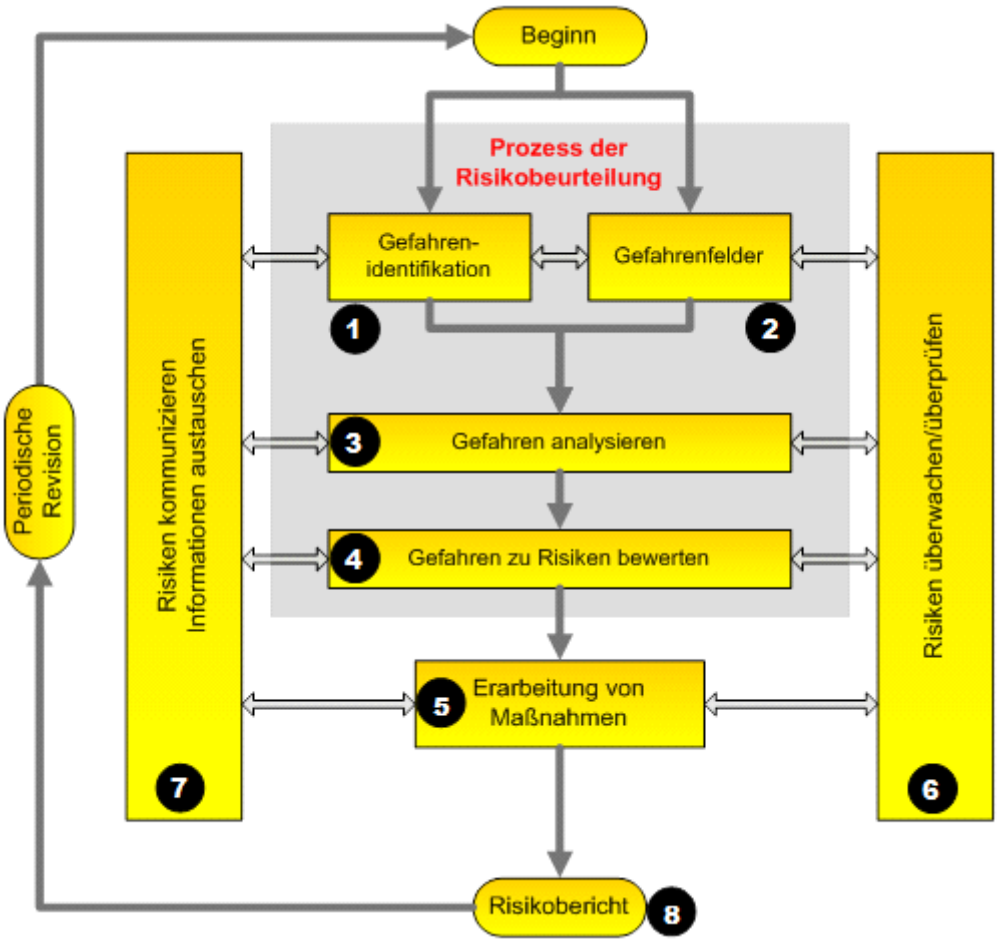


Abbildung 1: Vorgehensweise in der Risikoanalyse

3.1 Prozessschritt 1, Gefahrenidentifikation

Der Gefahrenidentifikationsprozess geht davon aus, dass Kommunikation in Form von Sprache und Daten in den Eigenschaften:

- Verfügbarkeit
- Vertraulichkeit und
- Integrität

gestört werden kann bzw. wird. Als wesentlichster Schritt wird die Erarbeitung eines umfassenden technisch-organisatorischen Kommunikationsgeflechts aller Marktteilnehmer in der Elektrizitätswirtschaft angesehen. Die Visualisierung wurde auf Basis der NIST „Guidelines for Smart Grid Cyber Security: Vol1, Smart Grid Cyber Security Strategy, Architecture and High-Level Requirements"[5] begonnen, mit den Festlegungen aus ebIX „Business Requirements and Information Models" Vorgaben[6] zusammengeführt und an die spezifischen Gegebenheiten der österreichischen E-Wirtschaft angepasst.

3.2 Prozessschritt 2, Gefahrenfelder

Die im Prozessschritt 1 erarbeiteten technisch-organisatorischen Kommunikations-beziehungen wurden in 15 verschiedene Bereiche eingeteilt. Diese 15 Bereiche wurden für die systematische Identifikation von Gefahren herangezogen. Somit wurden aus allen Kommunikationsbeziehungen 15 „Gefahrenfelder" oder Bereiche definiert.

3.3 Prozessschritt 3, Gefahrenanalyse

In den jeweiligen Gefahrenfeldern wurden aus folgenden Quellen mehr oder weniger aggregierte Einzelgefahren identifiziert bzw. diesen zugeordnet:

- NIST „Guidelines for Smart Grid Cyber Security Vol1" High Level Requirements
- BSI: Grundschutzkatalog[7]
- BSI: Sicherheit von Standleitungen[8]
- BSI: Technische Richtlinie BSI TR-03109-1 bis TR-03109-5 [9]
- Oesterreichs Energie, Security im Smart Grid, Bericht (TLP-AMBER)[10]

[5] Siehe Lit. ECA-27, NIST Guidelines for Smart Grid Cyber Security: Vol1, Smart grid Cyber Security Strategy, Architecture and High-Level Requirements"

[6] Siehe Lit. ECA-0X, ebIX, Business Requirements and Information Models

[7] Siehe Lit. ECA-06, BSI-Grundschutzkatalog

[8] Siehe Lit. ECA-09, BSI-Sicherheit von Standleitungen

[9] Siehe Lit. ECA-01, BSI: Technische Richtlinie BSI TR-03109-1 bis 5 (z.T. auch Drafts)

In Summe wurden 114 verschiedene Einzelgefahren zusammengestellt und in weiterer Folge analysiert.

3.4 Prozessschritt 4, Bewertung von Risiken

Das Risiko wird als Produkt von Eintrittswahrscheinlichkeit x Auswirkung definiert. Die Bewertung von Gefahren zu Risiken ist in folgenden Phasen erfolgt:

- Phase I, Festlegung der Bewertungskriterien, Eintrittswahrscheinlichkeit und Auswirkungsdimension (vgl. dazu auch Abschnitt 9)
- Phase II, Bewertung der 114 identifizierten Gefahren zu 73 Einzelrisiken, wobei die Risiken in mehrfacher Hinsicht bewertet wurden, einerseits einmal in der reinen Bewertung der Dimension des Stromausfalls und einmal mit Blick auf den Datenschutz (aus diesem Blickwinkel heraus betrachtet primär in reputativer Hinsicht). Andererseits wurde die Verteilung der Bewertung durch Betrachtung von Extremfällen „best-case“ und „worst-case“ sowie mit Blick auf einen „Erwartungswert“, dem „most-likely“- Fall berücksichtigt.
- Phase III, Aggregation der 73 Einzelrisiken zu 19 Aggregationsrisiken

3.5 Prozessschritt 5, Erarbeitung von Maßnahmen

Als Grundlage für die Erarbeitung von Maßnahmen wurde der „worst-case“ Fall herangezogen. Es wurde grundsätzlich versucht, bei allen Einzelrisiken sowie auch bei den Aggregationsrisiken Maßnahmen zur Risikominimierung zu erheben. Risiken, die in der „worst-case“ Betrachtung über der Risikotoleranzgrenze liegen, werden prioritär behandelt.
Gemäß den Vorgaben der ÖNORM S2410 wurde eine formal definierte Risikotoleranzgrenze festgelegt (rote Linie, rechte Abbildung).

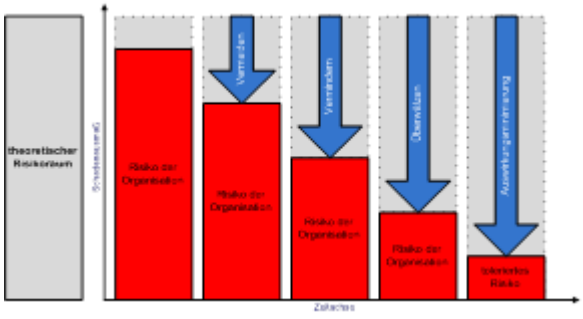


Abbildung 2: Allgemein definierte Risikopolitik gemäß ÖNORM S2410

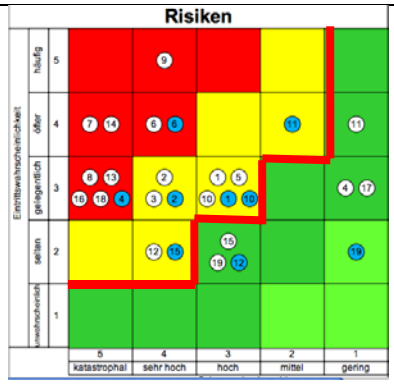


Abbildung 3: Risikotoleranzgrenze

[10] Siehe Lit.ECA-37, Oesterreichs Energie, Security im Smart Grid, Bericht(TLP-AMBER)

3.6 Prozessschritt 6, Risiken überprüfen

Alle Einzelrisiken und auch die Aggregationsrisiken sowie die Maßnahmenempfehlungen wurden iterativ in der Projektgruppe diskutiert und abgestimmt. Somit wurde ein Prozess der Risikokommunikation und des Erfahrungs- und Informationsaustausches innerhalb der Projektgruppe initiiert.

3.7 Prozessschritt 7, Risikobericht

Der vorliegende Risikobericht fasst den abgestimmten Sachstand mit 31.10.2013 zusammen.

3.8 Prozessschritt 8, Periodische Revision

Ex ante soll bzw. wird eine periodische Revision des Risikoberichts angeregt. Die Risikoänderungen durch Umsetzung von Maßnahmen sollten entsprechend erfasst werden, um den kontinuierlichen Verbesserungsprozess (KVP) zu dokumentieren.

4 Literaturzusammenstellung – und Recherchemöglichkeiten

Die vorliegende Risikoanalyse stellt umfassende Literatur zusammen. Der Bericht verweist auf die in der Quellensammlung zusammengestellten Literaturstellen wie folgt:

Lit.ECA-01, wobei die „01“ eine fortlaufende Nummer darstellt.

- „Lit.“ steht dabei für Literatur
- „ECA“ ist eine Infraprotect interne Abkürzung für den Bericht

Bei Anfragen von Kunden ermöglicht dies den direkten Zugriff auf nicht als Datei zur Verfügung gestellte klassifizierte oder urheberrechtlich geschützte Literatur.
Das entsprechende wissenschaftliche Zitat kann über die Suchfunktion auf der beiliegenden CD-R direkt gesucht werden. Es kann auch nach Schlagworten recherchiert werden (interne, offline „Google Suche“, ausführbar auch ohne Zugriff aufs Internet. Bitte beachten Sie, dass durch Sicherheitseinstellungen Ihres Browsers die Suchfunktion eingeschränkt sein könnte).
Urheberrechtlich geschützte Werke, insbesondere Normen, werden lediglich zitiert. Frei verfügbare Literatur, wie z.B. Risikoanalyse der Schweizer zum Thema IKT-Sicherheit des Bundesamts für Bevölkerungsschutz werden als Dateien der Literaturzusammenstellung beigelegt (vgl. dazu auch Anhang 6: Übersicht der Quellen)

Teil II Kontexterfassung

5 Die Österreichische Sicherheitsstrategie

Österreich verwirklicht seine Sicherheitspolitik im Rahmen des Konzepts der „Umfassenden Sicherheitsvorsorge“ (USV). Diese zielt auf das systematische Zusammenwirken verschiedener Politikbereiche auf Basis einer Gesamtstrategie und der relevanten Teilstrategien ab. Ein umfassendes Lagebild aller Akteure und ein darauf aufbauendes gemeinsames Lageverständnis sind notwendige Grundlagen für sicherheitspolitische Entscheidungen auf nationaler und internationaler Ebene. Dabei sollen Synergien im Sicherheitsbereich im Rahmen eines gesamtstaatlichen „Sicherheitsclusters“ erzielt werden.
Die im Juli 2013 beschlossene „Österreichische Sicherheitsstrategie“ betrachtet das Thema Sicherheit aus den Blickwinkeln der inneren Sicherheit, der Außenpolitik und der Verteidigungspolitik.
Das Thema Cybersecurity wird in dieser Strategie explizit mehrmals angesprochen.
Abgeleitet von der USV werden in Österreich daher parallel mehrere Teilstrategien, Sicherheits- und Schutzkonzepte entwickelt.

5.1 APCIP, Österreichisches Programm zum Schutz Kritischer Infrastrukturen

In der Genese einer neuen Sicherheitskultur in Österreich steht das aus dem Europäischen Programm „Schutz Kritischer Infrastrukturen“ (EPCIP) abgeleitete Österreichische Programm (APCIP) zum Schutz strategisch wichtiger Unternehmen in Österreich (APCIP).
Als eine Umsetzung der Vorgaben des APCIP wird die Entwicklung der IKT-Sicherheitsstrategie angesehen.

5.2 IKT-Sicherheitsstrategie

Im Frühjahr 2012 wurde durch das Bundeskanzleramt (BKA) gemeinsam mit Expertinnen und Experten aus Wirtschaft, Wissenschaft und öffentlicher Verwaltung eine IKT Sicherheitsstrategie entwickelt. Diese Strategie hat als Kernziele die kritischen Informationsinfrastrukturen und deren Schutz und fordert davon ausgehend die Umsetzung von Maßnahmen zur Festigung und Handlungsschemata, die die Kalkulierbarkeit der Risiken sicherstellen (Risikomanagement und Lagebild). Weitere Schwerpunkte sind die Themen Bildung und Forschung sowie das Thema Awareness.
Im Kontext zur Risikoanalyse der Informationssysteme der Energiewirtschaft sind vor allem die Vorgaben für den Schutz Kritischer Infrastrukturen relevant.
Es wird die Förderung des Risikomanagements innerhalb der Kritischen Infrastruktur explizit gefordert. Der Staat soll die Unternehmen dabei durch Maßnahmen wie Abgleich von

Informationen zur gemeinsamen Risikoanalyse, Akkreditierung von Risikomanagementmethoden, Angleichung von Ausbildungsmaßnahmen, Analysen der Technologiefolgenabschätzung und den Einsatz von Sanktionen und Anreizen unterstützen.
Weiter werden in diesem Bereich die Einrichtung eines Cyber-Krisenmanagements, der Aufbau eines Cyber-Lagezentrums und das Einrichten einer tragfähigen Krisenkommunikation gefordert. Das Cyber-Lagezentrum soll einen Überblick über die aktuelle Cyber-Situation ermöglichen und würde die bereits durch andere Einrichtungen (z.B. CERTs) wahrgenommenen Aktivitäten an einer zentralen Stelle bündeln. Bezüglich der Krisenkommunikation beschreibt die Strategie, dass sie gemeinsam durch gesicherte private und öffentliche Kommunikationsanlagen aufrechterhalten werden soll.
Das Thema Risikomanagement wird in diesem Bereich nochmals betrachtet, allerdings vor allem aus dem Blickwinkel der Forderung nach sektorübergreifenden Maßnahmen sowie der Sicherstellung von Mindeststandards. Die Motivation dafür entsteht aus der Einschätzung, dass jeder Sektor für sich ein gut ausgeprägtes Risikomanagement hat, eine übergreifende Risikobetrachtung aber fehlt. Eine zentrale Forderung der Strategie ist daher auch hier die Forderung nach einem Cyber-Lagezentrum.
In Bezug auf die Etablierung von Mindeststandards erwartet die Strategie eine Diskussion dazu, in welcher Form Mindeststandards verankert werden können (als Gesetze, Richtlinien, Normen, etc.) und zur Kontrolle der Einhaltung. Durch Umsetzung dieser Mindeststandards soll vor allem vermieden werden, dass aufgrund betriebswirtschaftlicher Überlegungen auf eine Risikovorsorge verzichtet wird.

5.3 Cybersecurity Risikoanalyse

Mit der Erstellung dieser Matrix wurde das Kuratorium Sicheres Österreich (KSÖ) beauftragt. Die Risikomatrix stellt einen Themenkatalog von 2011 zu aktuellen Cyberrisiken und eine Bewertung dieser Risiken nach Eintrittswahrscheinlichkeit und Auswirkung dar.
Da dieses Ergebnis alleine noch keinen Schluss auf notwendige Maßnahmen erlaubte, wurde ausgehend von der Matrix eine Cybersecurity-Risikoanalyse durch Interviews mit ausgewählten Unternehmen erstellt und eine Trennung in Unternehmenssektoren (Finanz, IKT, Energie, Transport, Behörden) vorgenommen.
Dem **Thema „Energieversorgung“ kam dabei eine besondere Rolle zu**, da es als essentiell für das Funktionieren der IKT-Systeme gesehen wurde und Angriffe auf die Energieversorgung als Bedrohung Nummer Eins aus der Cybersecurity Analyse hervorgingen.
Als Maßnahmen-Ergebnis fordert die Analyse die Umsetzung von fünf Handlungserfordernissen:

- Verständnis

- Erkennung und Bewertung von Cyberrisiken
- die systematische Organisation von Zusammenarbeit
- Förderung von Bewusstsein und Qualifikation der Nutzer,
- Stärkung von Cyberprävention und die Förderung von Verhaltensanreizen.

5.4 Zusammenführung in die ÖSCS

Die Ergebnisse der IKT-Sicherheitsstrategie und der Cybersecurity Initiative des BM.I wurden in einer Kooperation des Bundeskanzleramtes, des Verteidigungsministeriums und des Innenministeriums zur Erstellung einer nationalen Cybersecurity Strategie genutzt – der „Österreichischen Strategie für Cybersicherheit (ÖSCS)“.

Diese Strategie definiert unter anderem die Einrichtung einer Steuerungsgruppe und deren Zusammenarbeit mit privaten Akteuren aus Wirtschaft und Forschung, die Schaffung einer Struktur zur Koordination auf operativer Ebene und das bereits in der IKT Sicherheitsstrategie geforderte Cyber Krisenmanagement. Diese Strategie wurde im März 2013 beschlossen und aktuell sind mehrere interministerielle Arbeitsgruppen mit der Umsetzung befasst.

Die ÖSCS hat vor allem die Forderungen der IKT-Sicherheitstrategie nach einer Erstellung eines periodischen und anlassbezogenen „Lagebild Cyber Sicherheit“ und nach der Einbindung der Betreiber kritischer Infrastrukturen in die Prozesse des nationalen Cyber Krisenmanagements übernommen.

Auf rechtlicher Basis soll ein Bericht zu einem zeitgemäßen ordnungspolitischen Rahmen erstellt werden, der rechtliche Grundlagen und regulatorische Maßnahmen sowie nicht-rechtliche Selbstverpflichtungen prüft. Über eine gemeinsame Arbeit aller relevanten Stakeholder sollen Mindestsicherheitsstandards für Cybersicherheit definiert werden.

Zur Umsetzung der ÖSCS wurde eine interministerielle Steuerungsgruppe eingerichtet, die wiederum 4 interministeriellen Arbeitsgruppen die folgenden, aus der ÖSCS abgeleiteten, Teilaufgaben zugeordnet hat:

- Operative Koordinierung (Erstellung eines Lagebildes, Beratung über zu treffende Maßnahmen auf operativer Ebene, Schaffung einer Struktur, die als operatives Ausführungsorgan für ein übergreifendes Cyber Krisenmanagement genutzt werden kann)
- Erstellung eines Berichtes zum ordnungspolitischen Rahmen (rechtliche Grundlagen, regulatorische Maßnahmen, nicht-rechtliche Selbstverpflichtungen, Anreize und Sanktionen)

- Einrichtung einer Cyber Sicherheitsplattform (ständiger Informationsaustausch der öffentlichen Verwaltungen untereinander sowie der öffentlichen Verwaltung mit Vertretern der Wirtschaft, Wissenschaft und Forschung)
- Erstellung einer Kommunikationsstrategie (Abstimmung der bereits eingerichteten und geplanten staatlichen Websites)

Diese Arbeitsgruppen haben im Sommer 2013 ihre Arbeit aufgenommen und erste Ergebnisse bzw. Zwischenergebnisse werden im Frühjahr 2014 erwartet.

6 Auswertung bereits gewonnener/aktueller Erfahrungen in Österreich

6.1 Forschungsarbeiten in Österreich

Im Rahmen der Vorgespräche zu den Arbeitsworkshops wurde versucht, einen Überblick über die derzeitigen aktuellen Forschungsprojekte und Teststellungen zu gewinnen. Folgende Projekte wurden mit Blick auf die Aufgabenstellung näher betrachtet:

- BlackÖ.1, Das Projekt „Blackouts in Österreich“ analysiert die technischen, wirtschaftlichen und gesellschaftlichen Folgen von großflächigen Ausfällen im österreichischen Stromnetz.

- BlackÖ.2, Das Projekt Blackoutprävention und -intervention im österreichischen Stromnetz (BlackÖ.2) analysiert, aufbauend auf der im Kiras-Sicherheitsforschungsprojekt „Blackouts in Österreich“ (BlackÖ.1, 821746) erstellten Analyse des Status-quo des österreichischen Elektrizitätssystems, konkrete Lösungsvorschläge, wie die Versorgungssicherheit mit elektrischer Energie in Österreich auch in Zukunft sichergestellt werden kann.

- CAIS Im Projekt CAIS werden zwei Werkzeuge als Basis eines umfassenden Cyber Attack Information System zur Analyse und Bewertung von Bedrohungen im Cyberspace entwickelt.

- SG² – Smart Grid Security Guidance, Im Projekt SG2 werden systematische Untersuchungen von Smart Grid-Technologien in Bezug auf IKT-Sicherheitsaspekte und die Erforschung von effektiven Schutzmaßnahmen vor Cyber-Attacken durchgeführt. Aufbauend auf einer fundierten Bedrohungs- und Risikoanalyse aus einer gesamtstaatlichen Sicht und auf Sicherheitsanalysen von Smart Grid-Komponenten werden Maßnahmen für Stromnetzbetreiber erforscht, die zur Erhöhung der Sicherheit zukünftiger Computersysteme der Kritischen Infrastruktur "Stromversorgung" dienen.

6.2 Vorfall 02.-07.05.13

Am 2. Mai 2013 wurden ab ca. 15:20 Uhr erste Störmeldungen aus Leittechnikkomponenten von einzelnen Verteilernetzbetreibern und Kraftwerksbetreibern registriert. Als Störungsauswirkung wurden Einschränkungen und teilweise Ausfälle von Datenübertragungen festgestellt. Im Zuge der Fehleranalyse wurde eine auffällige

Netzbelastung durch Zählerabfragetelegramme identifiziert. Das initiale Fehlerbild wies sehr rasch auf ein „Kreisläuferproblem“ hin.

Im Zuge der Analyse der Bewältigung der Störung wurden die Stärken und Schwächen der österreichischen Eskalationskultur im Krisenmanagement eingehender betrachtet. Ergebnisse dieses Ereignisses wurden in den Risiken berücksichtigt.

6.3 Interministerielles Planspiel (KSÖ-Planspiel)

Die Maßnahmenforderungen der KSÖ Cybersecurity Analyse wurden im Anschluss an die Analysepräsentation im Rahmen eines Cyberplanspiels einer ersten Erprobung unterzogen. Dieses Planspiel war vor allem durch die gemeinsame Beteiligung von privaten Unternehmen und staatlichen Behörden zum damaligen Zeitpunkt einzigartig und zeigte vor allem wesentlichen Verbesserungsbedarf in der Kooperation zwischen den Beteiligten auf. Geprobt wurde das Verhalten der Spieler entsprechend ihrer eigenen Notfallszenarien bei einem großflächigen Internetausfall. Dieses Szenario war für alle Beteiligten eine sehr große Herausforderung, da die Abhängigkeit der Informationsübermittlung von Internet-Infrastrukturen inzwischen so groß geworden ist, dass alternative Wege und Prozesse nicht oder nicht mehr kurzfristig aktiviert werden können. In Bezug auf die E-Wirtschaft wurde vor allem die Übermittlung von Marktdaten per eMail als Risiko aufgezeigt. Der vorrangige Wunsch an die staatlichen Stellen war die Reaktivierung von Kommunikationswegen (z.B. über Funkverbindungen des Bundesheeres, etc.) bei Ausfall der eigenen Netze und die Einrichtung von „Single Points of Contact“ (SPOC) bei den Behörden.

6.4 CyberEurope CE.AT 2012

Initiiert durch die ENISA wurde im Oktober 2012 eine internationale Übung mit 27 europäischen Nationen durchgeführt. Szenar dabei war eine DDoS Attacke, die sich primär gegen Banken und Internet Service Provider gerichtet hat. Im Kontext zu dieser Risikoanalyse stehen dabei die identifizierten „Lessons Learned“ mit Blick auf die zeitlichen Abläufe der Bewältigung einer solchen Attacke, die einzusetzenden Instrumente der Erkennung und Abwehr in der nationalen und internationalen Kooperation zwischen staatlichen Stellen und der Privatwirtschaft, sowie aus den sich daraus ergebenden rechtlichen Fragestellungen. Im Rahmen dieser Übung wurden auch zum ersten Mal über alle teilnehmenden Organisationen hinweg KPIs[11] definiert, die den Übungserfolg messbar machen und zwischen den Teilnehmern einen objektivierten Vergleich erlauben.

[11] KPIs Key Performance Indikatoren

Die unterschiedliche Eskalationskultur zwischen Staat und Privatwirtschaft konnte anhand dieses Szenars ebenfalls dargestellt werden. Die Ergebnisse der Übung haben somit einen direkten Zusammenhang mit der Kollaborationskultur bei IKT-Störungen.

7 Internationaler Kontext

2006 wurde seitens der EU eine Initiative für eine sichere Informationsgesellschaft, die auf die „Entwicklung einer Kultur der Netz- und Informationssicherheit in Europa“ abzielte, entwickelt. 2009 wurde ein Programm zum Schutz kritischer Informationsinfrastrukturen (CIIP) begonnen, in deren Mittelpunkt der Schutz Europas vor Cyberstörungen durch eine Erhöhung der Sicherheitsvorkehrungen steht.

Neben den hier angeführten Strategien gibt es eine Vielzahl sehr konkreter Arbeitsgruppen, die sich mit dem Thema „Smart-Grid-Security“, Aufgabenstellungen, die den Herausforderungen der gegenständlichen Risikoanalyse sehr nahe kommen, beschäftigen.

In der Europäischen Agentur für Netz- und Informationssicherheit (ENISA) gibt es derzeit eine Arbeitsgruppe, Smart Grids Task Force 2012-2013. EG2[12], die folgende Ergebnisse erarbeiten will bzw. soll:

- Data Protection Impact Assessment (DPIA) template,
- a cybersecurity assessment framework,
- and minimum security requirements.

Die Risikoanalyse bezieht sich aber auch auf internationale Normungs- und Standardisierungsarbeit.

Eine sehr wichtige Rahmenbedingung für die vorliegende Risikoanalyse, insbesondere für die abzuleitenden Empfehlungen, ist die am 17.07.13 veröffentlichte ISO/IEC TR 27019:2013, Information technology -- Security techniques -- Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry.

Neben Strategien, laufenden Arbeitsgruppen, nationaler und internationaler Normen, gilt es auch noch bilaterale branchenspezifische Kooperationen im deutschsprachigen Raum zu berücksichtigen.

Stellvertretend werden hier die Ausführungshinweise zur Anwendung des BDEW Whitepapers „Anforderungen an sichere Steuerungs- und Telekommunikationssysteme“ zitiert[13].

[12] Siehe Lit.ECA-53, Appropriate security measures for smart grids, Guidelines to assess the sophistication of security measures implementation

[13] Siehe Lit. ECA-32, Anforderungen an sichere Steuerungs- und Telekommunikationssysteme

Teil III Ergebnisdarstellung der Risikoerfassung

8 Gefahrenidentifikation

Der Gefahrenidentifikationsprozess beruht im Wesentlichen darauf, dass Kommunikationsbeziehungen (technisch-organisatorischer Natur) dargestellt und analysiert wurden. Dazu wurden folgende Kommunikationsbeziehungen zusammengestellt und auf die österreichisch einzigartigen Gegebenheiten angepasst bzw. zu einem österreichweit gültigen Kommunikationsgeflecht zusammengeführt:

- NIST „Guidelines for Smart Grid Cyber Security Vol1" High Level Requirements"
- ebIX, "Introduction to Business Requirements and Information Models"[14]
- ECA-Beziehungsgeflecht zwischen Marktteilnehmern

8.1 Domänenmodell gemäß NISTIR 7628 Guidelines for Smart Grid Cyber Security

Ausgangspunkt der Kommunikationsbeziehungen ist eine Grobgliederung von Fachbereichen.

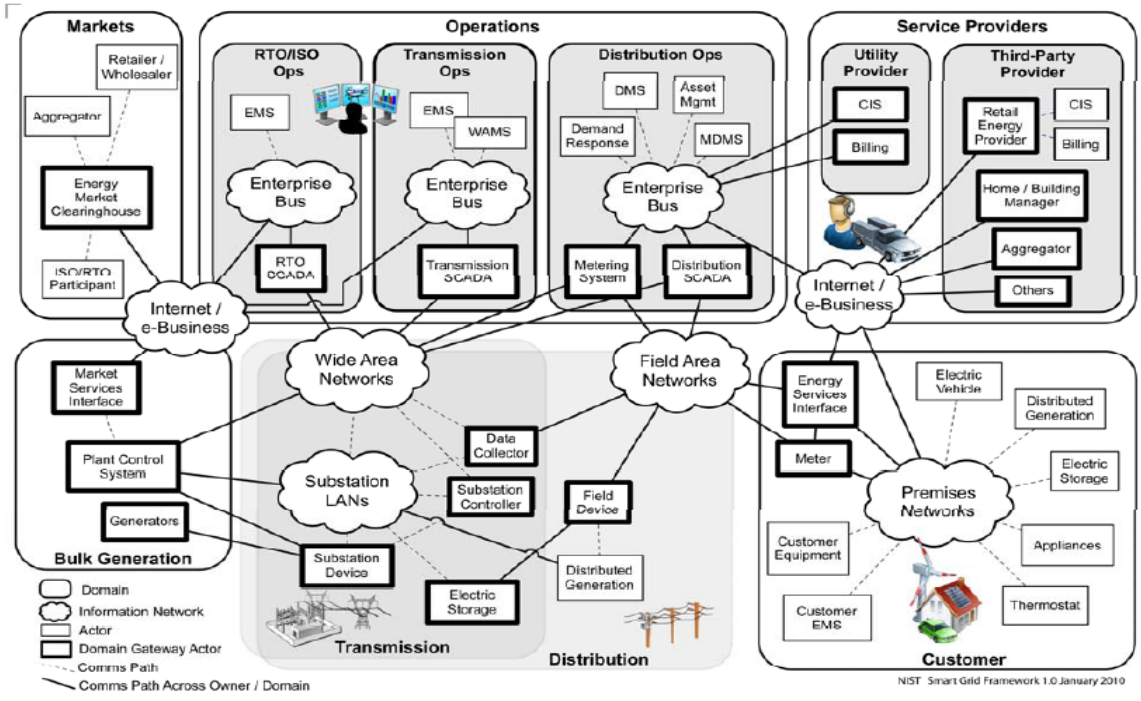


Abbildung 4: Domänenmodell, NISTIR 7628 Guidelines for Smart Grid Cyber Security

Eine Analyse der Kommunikationsbeziehungen zeigt, dass dieses Modell für Europa bzw. Österreich nicht 1:1 übernommen werden kann. Es ist aber eine gute Grundlage, um die Kommunikationsbeziehungen auf die österreichischen Bedürfnisse anzupassen.

[14] Siehe Lit.ECA-62, ebIX, Introduction to Business Requirements and Information Models"

8.2 Domänenmodell .AT

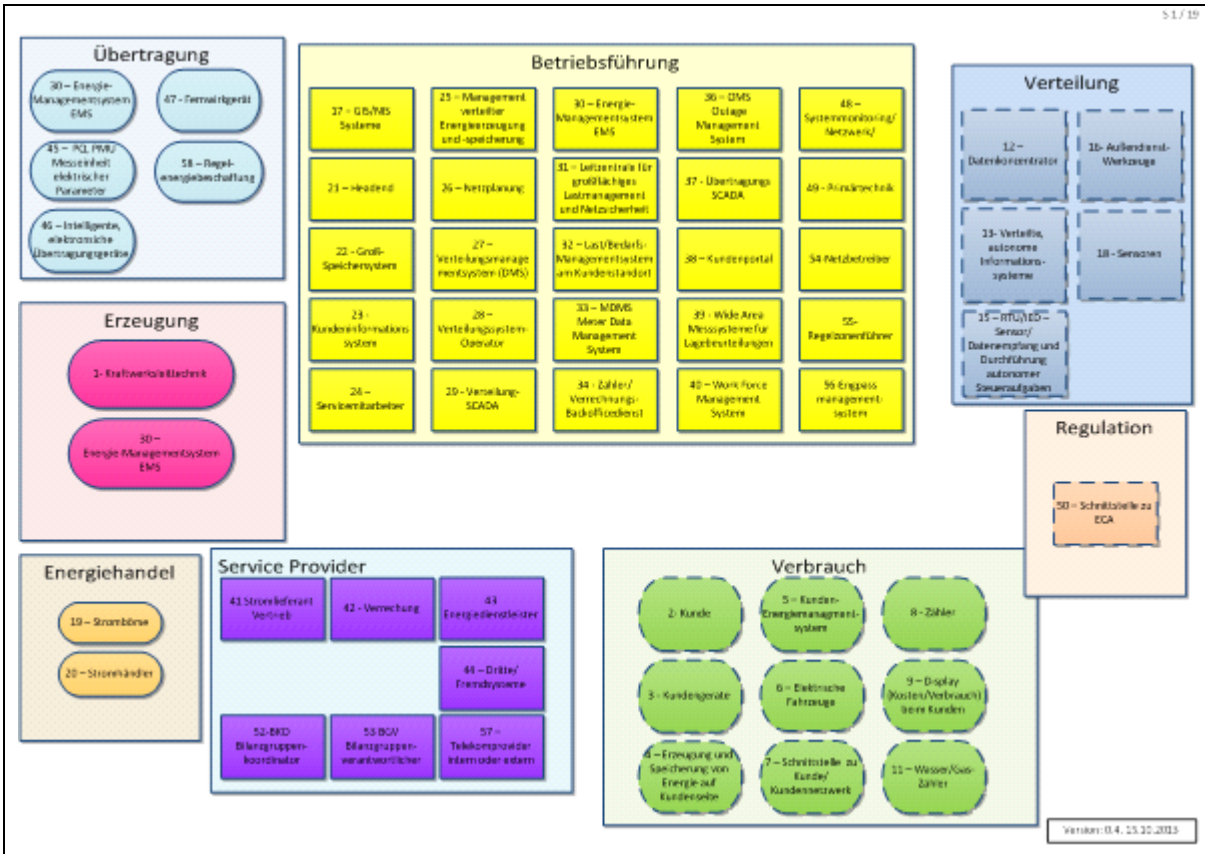


Abbildung 5: Arbeitsgruppierung kommunikativ-funktionaler Zusammenhänge

In Anlehnung bzw. abgeleitet aus dem NIST-Domänenmodell wurden folgende Gruppen funktionaler Einheiten zusammengefasst:

- Erzeugung
- Verteilung
- Übertragung
- Betriebsführung
- Energiehandel
- Verbraucher
- Regulation

Durch die Komplexität der technisch-organisatorischen Kommunikationsbeziehungen ist eine eineindeutige Zuordnung der einzelnen „funktionalen Einheiten“ in eine Domäne nicht immer möglich, da die funktionalen Einheiten zum Teil mit mehreren Domänen kommunizieren sollen/ dürfen/ müssen bzw. in mehreren Domänen vergleichbare Funktionen erfüllen. Dies sei am Beispiel 30-Energiemanagementsystem kurz erläutert. Diese Funktion gibt es in den Bereichen Erzeugung, Übertragung, Betriebsführung und eigentlich auch bei den

Verbrauchen, dort als eigene funktionale Einheit 5-Kundenenergiemanagementsystem aufgeführt. Abhängig von der betrachteten Netzebene, kann es unterschiedlichen Kommunikationsbedarf bzw. verschiedene Ausprägungen der Kommunikation geben. Da diese Art der Visualisierung kein technisches Schema (im Sinne Schaltbild, Blockdarstellung udg) darstellt, sondern primär ein Werkzeug, um „IKT-Interdependenzen“ zu identifizieren, wurde versucht, eine funktionale Einheit auch nur einmal im Gesamtkommunikationsgeflecht darzustellen.

Eine Kurzerklärung der „funktionalen Einheiten“ ist im Anhang 2: Kurzbeschreibung der funktionalen Einheiten zusammengestellt.

8.3 Übersicht über alle Kommunikationsbeziehungen

Die Kommunikationsbeziehungen wurden in 15 Bereiche, in weiterer Folge Gefahrenfelder genannt, abgebildet. Es sind dies:

- Gefahrenfeld I: Maschinen-Maschinen Kommunikation mit/ und /oder hohem Rechenaufwand/ und/ oder Bandbreitenanforderung
- Gefahrenfeld II: Gefahren an der Schnittstelle Steuerungs- und Kontrollsysteme innerhalb einer Organisation
- Gefahrenfeld III: Gefahren an der Schnittstelle Steuerungs- und Kontrollsysteme zwischen verschiedenen Organisationen
- Gefahrenfeld IV: Gefahren, die sich aus Back-Office-Systemen ableiten lassen. Innerhalb einer Organisation oder auch von und zu verschiedenen Netzbetreibern.
- Gefahrenfeld V: Gefahren, die sich aus interorganisatorischer Kommunikation (z.B. Fahrplanmanagement) ableiten lassen.
- Gefahrenfeld VI: Gefahren, die sich aus Schnittstellen zwischen Steuerungssystemen und Verwaltungs- und Administrationssystemen ableiten lassen
- Gefahrenfeld VII: Gefahren, die sich aus Schnittstellen Sensor-Sensornetzwerk und Überwachungstechnik ableiten lassen.
- Gefahrenfeld VIII: Gefahren, die sich aus Schnittstellen im Smart Meter Netzwerk ableiten lassen.
- Gefahrenfeld IX: Gefahren, die sich aus der Nutzung von Kunden HAN/BAN/NAN Netzwerken ableiten lassen.
- Gefahrenfeld X: Gefahren, die sich aus der Nutzung externer Systeme ableiten lassen, die eine "direkte" Beziehung zum Endverbraucher haben.
- Gefahrenfeld XI: Gefahren, die sich aus Service- und Wartungsschnittstellen ableiten lassen.

- Gefahrenfeld XII: Gefahren, die sich aus den Schnittstellen am Smart Meter ableiten lassen.
- Gefahrenfeld XIII: Gefahren, die sich aus der Nutzung von Decision Support Systemen ableiten lassen.
- Gefahrenfeld XIV: Gefahren, die sich aus der Schnittstelle Entwicklung/ Wartung an der Sekundärtechnik ableiten lassen.
- Gefahrenfeld XV: Gefahren, die sich aus der Nutzung von Netzwerküberwachung und Securitymonitoring-Systemen ableiten lassen.

8.4 Zuordnung von Einzelgefahren zu den Gefahrenfeldern

In den 15 Gefahrenfeldern wurden einzelne Gefahren ausformuliert. Diese Gefahren wurden einerseits in 5 Workshops erarbeitet und zum Teil aus den folgenden Katalogen bzw. Studien entnommen:

1. NIST „Guidelines for Smart Grid Cyber Security Vol1" High Level Requirements"
2. BSI: Grundschutzkataloge, Standleitungssicherheit, Schutzprofile etc
3. Risikoanalyse Öesterreichs Energie, Smart Grid Security

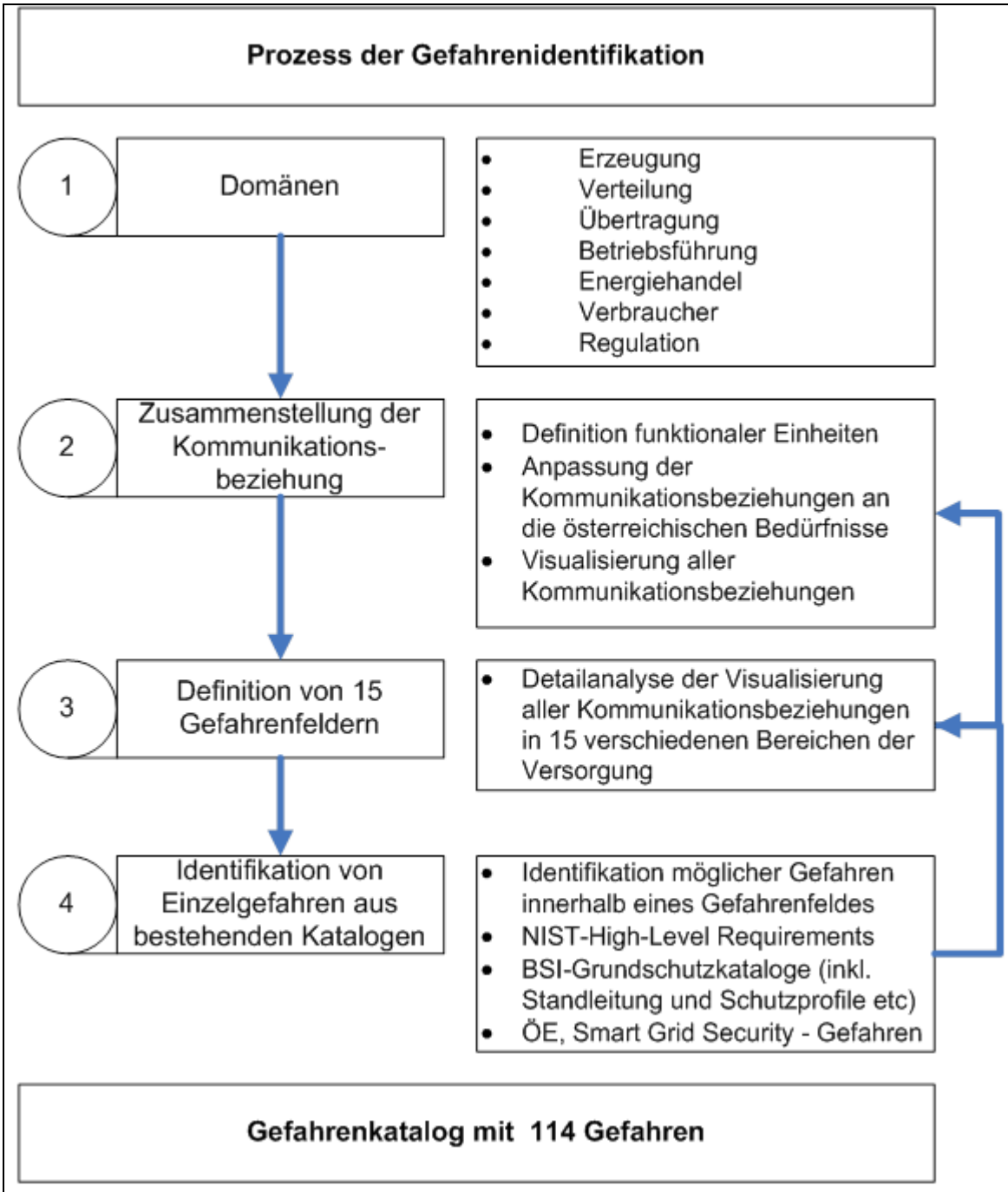


Abbildung 6: Prozess der Gefahrenidentifikation

8.5 Gefahrenkatalog gesamt

Wie man anhand der Zuordnung von Einzelgefahren zu den 15 Gefahrenfeldern leicht erkennen kann, werden Einzelgefahren mehrfach in den Gefahrenfeldern genannt.

Im letzten Schritt des Gefahrenidentifikationsprozesses (vgl. dazu Abbildung 6) wurden die Einzelgefahren in einem Gesamtkatalog zusammengefasst. Siehe dazu Anhang 3: Gefahrenkatalog gesamt.

Der grundsätzliche Aufbau wird anhand eines Beispiels dargestellt. Spalte A, laufende Nummer, Spalte B die Beschreibung der Gefahr, in Spalte C ist erfasst, zu welchen Gefahrenfeldern die Einzelgefahr zugeordnet werden kann.

A	B	C														
Nr.	**Gefahrenbeschreibung**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
1	Gefahr einer absichtlichen, aber nicht autorisierten Auslösung von Schalthandlungen, die keine User Identifizierung oder Authentifizierung benötigen	X	X	X												
2	Gefahr, dass Unbefugte Zugang zu nicht privilegierten Remote-Access-Accounts, LAN-Accounts mit Privilegien oder Remote- Access-LAN- Accounts mit Privilegien erhalten	X	X	X	X	X	X		X	X	X	X	X		X	X

Tabelle 4: Aufbau des Gefahrenkatalogs

9 Risikobewertungskriterien

Um identifizierte Gefahren zu Risiken zu bewerten, bedarf es vereinheitlichter Bewertungskriterien. Dazu wurde ein Bewertungsschema mit Punkten in der Projektgruppe abgestimmt. Dies wurde sowohl für die Eintrittswahrscheinlichkeit als auch für die Auswirkungsdimension entsprechend behandelt.

9.1 Allgemeines zur Herleitung der Bewertungskriterien

Die Bewertungskriterien wurden dabei in mehreren Schritten erarbeitet. In einem ersten Schritt wurden die Ergebnisse der Schweizer Risikoanalyse im Bereich ICT-Infrastruktur, Sektor elektrische Energie[15], zur Abstufung der nicht zeitgerecht gelieferten Energie und zur Einschätzung der Eintrittswahrscheinlichkeit sowie zur Definition eines relevanten Stromausfalls ausgewertet.

Die schweizer Risikoanalyse berücksichtigt primär Aspekte des Übertragungsnetzes und konnte nicht 1:1 für die Zielsetzungen der österreichischen Risikoanalyse herangezogen werden.

[15] Siehe Lit. ECA-44, Risikoanalyse Bereich ICT-Infrastruktur

Die Rahmenbedingungen für einen *nennenswerten flächendeckenden* Stromausfall für Österreich sind noch nicht definiert. Um der Aufgabenstellung gerecht zu werden, wurde in einem zweiten Schritt nach einer flexiblen und für alle „Netzbetreiber“ allgemein gültigen Festlegung für die Bewertungen von Gefahren gesucht. Dazu wurden folgende Rahmenbedingungen formuliert:

- Für das Bewertungskriterium „Eintrittswahrscheinlichkeit“ soll eine für alle „Netzbetreiber“[16] einheitliche Definition bzw. Abstufung gefunden werden
- Es soll eine klare Unterscheidung zwischen Eintrittswahrscheinlichkeiten bei technischen Gefahren und Naturgefahren und der Machbarkeit als Maß der „Eintrittswahrscheinlichkeit“ für intentionale Gefahren geben, um den Gegebenheiten von „Cyberattacken“ entsprechend Rechnung tragen zu können.
- Für das Bewertungskriterium „Auswirkung“ soll eine für alle Netzbetreiber einheitliche Definition und Abstufung gefunden werden, die jedoch die spezifischen Versorgungsaufgaben bzw. Gegebenheiten der einzelnen Netzbetreiber in absoluten Zahlen und unterschiedlichen Dimension berücksichtigt
- In Summe soll die Relation der verschiedenen IKT-Risiken zueinander eine 1:1 Vergleichbarkeit zwischen den unterschiedlichen Netzbetreibern ermöglichen. Damit soll auch eine individuelle Fortschreibung des Identifikations- und Bewertungsprozesses von Risiken bei allen „Netzbetreibern“ gewährleistet werden.

Für die Bewertung der Schadensdimension (nennenswerter flächendeckender Stromausfall) wurden die von der E-Control definierten vier Status der Versorgung als Grundlage herangezogen:

- Normalbetrieb / Normal Operation
- Gefährdeter Normalbetrieb / Alert
- Gestörter Betrieb / Emergency
- Großstörung / Blackout

9.1.1 Grundlagen für die Bewertung der Schadensdimension

9.1.1.1 Normalbetrieb / Normal Operation

Ein sicherer Normalbetrieb liegt vor:

- wenn alle Kunden versorgt werden

[16] Übertragungsnetz, Verteilnetz udg.

- alle Grenzwerte eingehalten werden, also z.B. keine Überlastungen von Betriebsmitteln und keine Spannungsüber- oder Unterschreitungen auftreten und ausreichende Kraftwerks- und Übertragungsreserven vorhanden sind und
- das (n–1)-Kriterium in einem Netz mit einer Nennspannung ≥ 110 kV überall erfüllt ist.

Auch im Falle von isolierten Ereignissen im Netz, wie z.B. Betriebsmittelausfällen, die keine unmittelbaren Auswirkungen auf den Netzbetrieb haben bzw. durch betriebliche Maßnahmen kompensiert werden können, spricht man weiter von Normalbetrieb.

9.1.1.2 Gefährdeter Normalbetrieb / Alert

Ein gefährdeter Normalbetrieb liegt vor:

- wenn alle Kunden versorgt werden
- wenn das System zwar nach wie vor stabil ist und alle Grenzwerte eingehalten werden, jedoch für die Gewährleistung eines sicheren Betriebs erforderliche Betriebsreserven bereits aufgebraucht sind.
- wenn das (n-1)-Kriterium in einem Netz mit einer Nennspannung ≥ 110 kV nicht überall erfüllt ist.

9.1.1.3 Gestörter Betrieb / Emergency

Ein gestörter Betrieb liegt vor:

- wenn eine instabile bzw. sich verschlechternde Situation gegeben ist
- Grenzwerte (z.B. für Spannung, Frequenz sowie Leistungswerte bei Betriebsmitteln) nicht mehr eingehalten werden können; es können bereits beschränkte Versorgungsunterbrechungen auftreten
- Sicherheitsgrenzen, wie das (n1)-Kriterium in Netzen mit einer Nennspannung ≥ 110 kV, werden nicht mehr eingehalten.
- trotz entsprechender Abhilfemaßnahmen (z.B. Lastanpassung) kann eine Störungsausweitung nicht ausgeschlossen werden.

9.1.1.4 Großstörung / Blackout

Eine Großstörung liegt vor bei Spannungslosigkeit:

- im gesamten Übertragungsnetz eines Netzbetreibers oder
- in mehreren Netzen benachbarter Netzbetreiber oder
- in Netzteilen eines oder mehrerer benachbarter Übertragungsnetze oder
- in Verteilernetzen

und erfordert einen Netzwiederaufbau.

Im Hinblick auf die Eintrittswahrscheinlichkeit von technischen Gebrechen und Naturgefahren kann man auf die Daten der Ausfalls- und Störungsstatistik[17] der E-Control zurückgreifen.

[17] Siehe Lit. ECA-16, Ausfalls- und Störungsstatistik

9.2 Festlegung der Eintrittswahrscheinlichkeiten und Machbarkeit

9.2.1 Technische Gebrechen und Naturgefahren

Technische Gefahren- und Naturgefahren			
Eintritts-wahrscheinlichkeit	**Verbale Beschreibung**	**Mind. Häufigkeit 1 mal pro**	**Bewertung Punkte**
unwahrscheinlich	Das Ereignis bzw. die Gefahr ist unwahrscheinlich und tritt einmal in 50 Jahren auf.	50 Jahren	**1**
selten	Das Ereignis bzw. die Gefahr ist selten und tritt langfristig einmal in 20 Jahren auf.	20 Jahren	**2**
gelegentlich	Das Ereignis bzw. die Gefahr ist denkbar und tritt mittelfristig einmal in 10 Jahren auf.	10 Jahren	**3**
öfters	Das Ereignis bzw. die Gefahr ist möglich und tritt kurzfristig einmal in 1-5 Jahren auf.	5 Jahren	**4**
häufig	Das Ereignis bzw. die Gefahr ist bekannt und tritt unterjährig auf.	Jahr oder öfter	**5**

Tabelle 5: Bewertung der Eintrittswahrscheinlichkeit technische und Naturgefahren

9.2.2 Festlegung der Machbarkeit; „Eintrittswahrscheinlichkeiten“ für intentionale Gefahren

Machbarkeit Intentionale Gefahren			
Eintritts-wahrscheinlichkeit	**Verbale Beschreibung**	**Aufwand in Zeit und Know-how**	**Bewertung Punkte**
unwahrscheinlich	Sehr hoher Aufwand für die Tatausführung. Setzt Wissen voraus, das man sich durch sehr intensive Beschäftigung mit der Materie über einen längeren Zeitraum aneignen muss. Die Tat setzt auch voraus, dass man physische und organisatorische Barrieren unentdeckt überwinden kann.	Wochen - Monate der Vorbereitung/ Expertenniveau	**1**
selten	Hoher Aufwand für die Tatausführung. Setzt Wissen voraus, das man sich durch intensive Beschäftigung mit der Materie aneignen kann. Die Tat setzt voraus, dass man physische und organisatorische Barrieren (auch soziale Kenntnisse) unentdeckt überwindet.	Wochen der Vorbereitung - spezielle Fachkenntnisse werden vorausgesetzt	**2**
gelegentlich	Überschaubarer Aufwand für die Tatausführung. Das Ziel hat subjektiv eine gewisse Attraktivität. Die Tat setzt voraus, dass man physische Barrieren überwinden muss.	Tage der Vorbereitung- Fachkenntnisse werden vorausgesetzt	**3**

Machbarkeit Intentionale Gefahren			
Eintritts-wahrscheinlichkeit	**Verbale Beschreibung**	**Aufwand in Zeit und Know-how**	**Bewertung Punkte**
öfters	Geringer Aufwand für die Tatausführung. Das Ziel hat eine subjektiv hohe Attraktivität. Die Tat setzt voraus, dass IKT-basierte Barrieren überwunden werden müssen. Für die Tatausführung müssen jedoch eigene Werkzeuge geschaffen werden.	Wenige Tage der Vorbereitung werden vorausgesetzt.	**4**
häufig	Sehr geringer Aufwand für die Tatausführung. Das Ziel hat eine subjektiv hohe Attraktivität. Die Tat setzt voraus, dass IKT-basierte Barrieren überwunden werden müssen.	Es stehen bereits anpassbare Werkzeuge bzw. Werkzeugkisten zur Verfügung. Die Tat kann von interessierten Laien begangen werden.	**5**
Der Aufwand wird auch finanziell verstanden			

Tabelle 6: Bewertung der „Eintrittswahrscheinlichkeit“ intentionaler Gefahren

9.3 Bewertungskriterien der Auswirkungsdimensionen

Bewertung der Auswirkungen von Gefahren			
Auswirkung	**Verbale Beschreibung quantifizierend**	**Verbale Beschreibung qualitativ-reputativ**	**Bewertung Punkte**
gering	Es sind mehr als 1 % der Anschlüsse im betrachteten Versorgungsgebiet von einer Stromunterbrechung für ca. 30 Min. betroffen. 1% der Peak Netz/Netz-Last des EVUs ist betroffen.	Versorgungsausfälle wie sie normalerweise auftreten können. Störung eines kleinen Teilnetzes (Abzweig) - kein reputativer Schaden	**1**
mittel	Es sind mehr als 2 % der Anschlüsse im betrachteten Versorgungsgebiet von einer Stromunterbrechung für ca. 1h betroffen. 2% der Peak Netz/Netz-Last des EVUs ist betroffen.	Ereignis bedingt organisatorisch-technischen Veränderungsbedarf in der IKT-Infrastruktur - geringer reputativer Schaden	**2**
hoch	Es sind mehr als 10 % der Anschlüsse im betrachteten Versorgungsgebiet von einer Stromunterbrechung für ca. 3h betroffen. 10% der Peak Netz/Netz-Last des EVUs ist betroffen.	Ereignis bedingt erheblichen organisatorisch-technischen Veränderungsbedarf in der IKT-Infrastruktur mit erheblichen personellen und finanziellen Ressourcen - reputativer Schaden, der nennenswerte finanzielle Ressourcen bindet um korrigiert zu werden	**3**

Bewertung der Auswirkungen von Gefahren			
Auswirkung	**Verbale Beschreibung quantifizierend**	**Verbale Beschreibung qualitativ-reputativ**	**Bewertung Punkte**
sehr hoch	Es sind mehr als 20 % der Anschlüsse im betrachteten Versorgungsgebiet von einer Stromunterbrechung für ca. 6h betroffen. 20% der Peak Netz/Netz-Last des EVUs ist betroffen.	Ereignis bedingt grundsätzliche organisatorisch-technische Veränderungen, da eine ausgenutzte Schwachstelle aufgrund der eingesetzten Hard- und Software nicht mittelbar geschlossen werden kann. Es existieren jedoch organisatorische Maßnahmen, welche die Schwachstellen überwachen und auswirkungsminimierende Maßnahmen können gesetzt werden. Sehr hoher reputativer Schaden	**4**
katastrophal	Es sind mehr als 50 % der Anschlüsse im betrachteten Versorgungsgebiet von einer Stromunterbrechung für ca. 12h betroffen, auch Totalausfall.	Ereignis bedingt grundsätzliche organisatorisch-technische Veränderungen, da eine ausgenutzte Schwachstelle aufgrund der eingesetzten Hard- und Software nicht mittelbar geschlossen werden kann. Katastrophaler reputativer Schaden	**5**
Für die Bewertung des „Schadens“ wird ein logisches „oder“ herangezogen und das für das EVU wichtigste Kriterium ausgewählt			

Tabelle 7: Bewertung der Schadensdimension

Für die Bewertung des Schadensausmaßes wurden zwei Bewertungsskalen ermöglicht. Die erste Skala beschäftigt sich ausschließlich mit der Dimension eines möglichen Stromausfalls. Hier ist eine logische „oder“ Verknüpfung der verbalen Beschreibungen für die Festlegung der korrelierten Punkte bzw. in die Eingruppierung zwischen gering und katastrophal möglich.

Je nach Art der angenommenen Störung kann hier entweder eine definierte Anzahl an Kunden (Hausanschlüsse) oder eine definierte nicht zeitgerecht gelieferte „Energie“ ausgewählt werden. Die mögliche Schadensdimension wird entweder in einer Prozentzahl der maximalen „Netz/Netz-Last“ durch den Netzbetreiber definiert oder durch die betroffenen „Haushaltsanschlüsse“ im betrachteten Versorgungsgebiet. Die angenommene Stromausfallsdauer ist hier ebenfalls mit abgestuft. Durch die Kombination dreier Parameter (Ausfallsdauer, betroffene ausgefallene Netz/Netz-Last und Anzahl der Hausanschlüsse) können so verschiedene nennenswerte Stromausfallsszenarien betreiber-unabhängig definiert werden. Die drei Parameter weisen in verschiedenen Szenarien unterschiedliche Abhängigkeiten auf, wurden jedoch in „repräsentative“ Eskalationsstufen (Auswirkung von gering - katastrophal) eingeteilt.

Die zweite Bewertungsskala eines möglichen Schadensausmaßes ist der mit einer Störung oder Ereignis verbundene reputative Image- oder Vertrauensverlust (zweite Spalte „Verbale Beschreibung qualitativ-reputativ“).

Wiederholend sei darauf hingewiesen, dass im Rahmen der Risikobetrachtung nur Gefahren bewertet werden, die einen nennenswerten Stromausfall durch den Einsatz der Informations- und Kommunikationstechnologie auslösen können. Ob die Ursache ein technischer Fehler, ein technisches Gebrechen, Naturgefahren oder aber auch durch kriminelle, vorsätzliche Handlungen bzw. Manipulationen von Menschen an der IKT bedingt ist, spielt nur bedingt eine Rolle.

In diesem Zusammenhang werden auch Aspekte des Datenschutzes bewertet. Während man bei Gefahren, die Integritätsverlust und Wegfall der Verfügbarkeit von Informationen und Daten ansprechen, sehr leicht einen direkten Zusammenhang zu einem möglichen Stromausfall herstellen kann, ist eine direkte Korrelation personenbezogener oder auch organisatorisch-betrieblich-vertraulicher Daten nicht immer zwingend darstellbar und unmittelbar.

Diese Gefahren werden ebenfalls in zweifacher Hinsicht bewertet. Einmal im unmittelbaren Zusammenhang mit einem möglichen Stromausfall und einmal mit primär reputativer Schadwirkung, da hier im Worst-Case Datenschutzverletzung und somit Gesetze verletzt werden könnten. Eine „Verletzung“ von Informationspflichten und eine mögliche Missachtung von Sorgfaltspflichten werden in diesem Kontext reputativen Risiken zugeordnet, da eine direkte Auswirkung auf die Versorgungssicherheit in diesem Zusammenhang nicht darstellbar ist.

9.4 Risikobewertungsprozess

Die Gefahren wurden in mehreren Arbeitsworkshops zu Risiken bewertet. Dazu wurden folgende Schritte festgeschrieben:

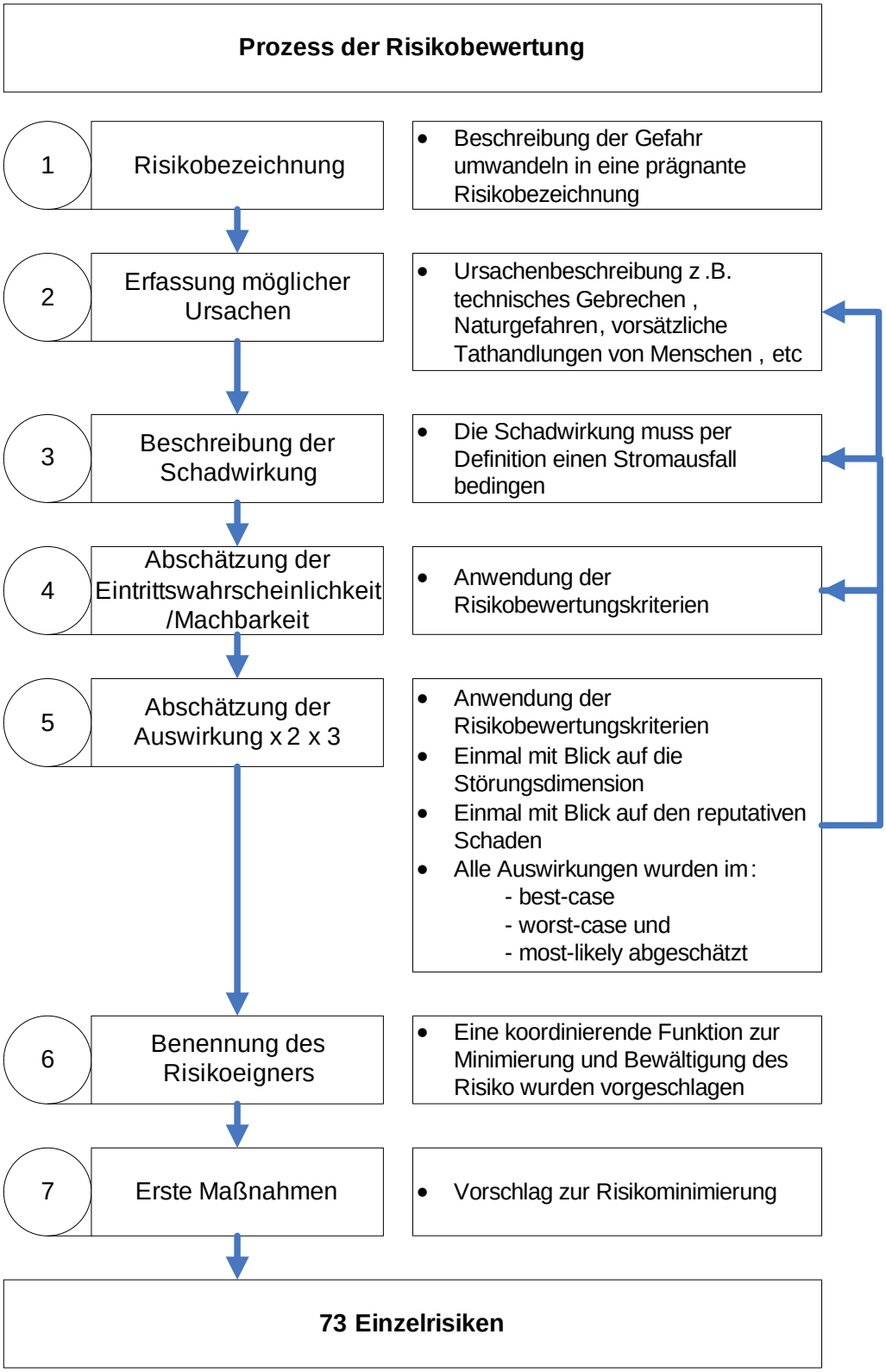


Abbildung 7: Prozess der Risikobewertung

9.5 Ergebnisdarstellung der Einzelgefahren Auflistung-Auszug

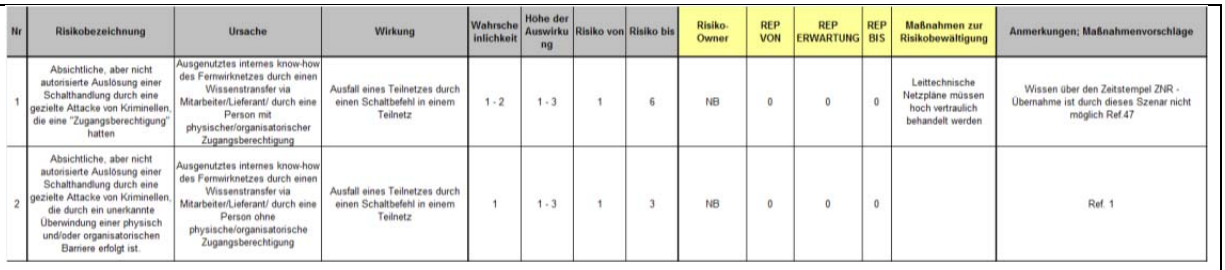
1	2	3	4	5
Risikobezeichnung	**Ursache**	**Wirkung**	**EW**	**AW**
Absichtliche, aber nicht autorisierte Auslösung einer Schalthandlung durch eine gezielte Attacke von Kriminellen, die eine "Zugangsberechtigung" hatten	Ausgenutztes internes know-how des Fernwirknetzes durch einen Wissenstransfer via Mitarbeiter/Lieferant/ durch eine Person mit physischer/organisatorischer Zugangsberechtigung	Ausfall eines Teilnetzes durch einen Schaltbefehl in einem Teilnetz	1 - 2	1 - 3

Fortsetzung der Tabelle

6	**5** (reputative Auswirkungen, best-case, most likely, worst-case)			7	Details und Anmerkung sowie Referenz zur Gefahr aus dem Gefahrenkatalog
Risiko-Owner	**REP VON**	**REP ERWARTUNG**	**REP BIS**	**Maßnahmen zur Risikobewältigung**	**Anmerkungen; Maßnahmenvorschläge**
NB	1	3	4	Leittechnische Netzpläne müssen hoch vertraulich behandelt werden	Wissen über den Zeitstempel ZNR - Übernahme ist durch dieses Szenar nicht möglich Ref.47

Tabelle 8: Risikobewertung

Gesamtübersicht:



Nr	Risikobezeichnung	Ursache	Wirkung	Wahrscheinlichkeit	Höhe der Auswirkung	Risiko von	Risiko bis	Risiko-Owner	REP VON	REP ERWARTUNG	REP BIS	Maßnahmen zur Risikobewältigung	Anmerkungen; Maßnahmenvorschläge
1	Absichtliche, aber nicht autorisierte Auslösung einer Schalthandlung durch eine gezielte Attacke von Kriminellen, die eine "Zugangsberechtigung" hatten	Ausgenutztes internes know-how des Fernwirknetzes durch einen Wissenstransfer via Mitarbeiter/Lieferant/ durch eine Person mit physischer/organisatorischer Zugangsberechtigung	Ausfall eines Teilnetzes durch einen Schaltbefehl in einem Teilnetz	1 - 2	1 - 3	1	6	NB	0	0	0	Leittechnische Netzpläne müssen hoch vertraulich behandelt werden	Wissen über den Zeitstempel ZNR - Übernahme ist durch dieses Szenar nicht möglich Ref.47
2	Absichtliche, aber nicht autorisierte Auslösung einer Schalthandlung durch eine gezielte Attacke von Kriminellen, die durch ein unerkannte Überwindung einer physisch und/oder organisatorischen Barriere erfolgt ist.	Ausgenutztes internes know-how des Fernwirknetzes durch einen Wissenstransfer via Mitarbeiter/Lieferant/ durch eine Person ohne physische/organisatorische Zugangsberechtigung	Ausfall eines Teilnetzes durch einen Schaltbefehl in einem Teilnetz	1	1 - 3	1	3	NB	0	0	0		Ref. 1

Abbildung 8: Risikobewertungsbogen

Nachfolgende Darstellung der Ergebnisse wird in folgenden Schritten aufgebaut:

1. Darstellung der Risikomatrix im „most-likely“, quantitative Darstellung (Schadensdimension Stromausfall)
2. Darstellung der Risikomatrix im „most-likely“, reputative Darstellung
3. Darstellung der Risikomatrix im „worst-case“, quantitative Darstellung (Schadensdimension Stromausfall)
4. Darstellung der Risikomatrix im „worst-case“, reputative Darstellung
5. Tabellarische Auflistung der Ergebnisse

10 Risikomatrix aller Einzelgefahren

Die Risikomatrix aller Einzelgefahren wurde mit Experten der Netzbetreiber und Stromerzeuger sowie mit Verantwortlichen aus den Ministerien erarbeitet und zusammengestellt. Aufgrund der Sensibilität der Aussagen der Risikomatrix steht die Auflistung der Einzelrisiken nur Fachexperten zur Verfügung.

11 Risikomatrix der Aggregationsrisiken

11.1 Aggregationsprozess

Die 73 Einzelrisiken wurden aus dem Gefahrenkatalog abgeleitet. Um diese Risiken auf ein überschaubares Maß zu reduzieren, wurden Risiken aus folgenden Gesichtspunkten bzw. Analysen heraus zusammengefasst:

- Ähnliche oder vergleichbare Ursachen inkl. vergleichbarer Tatmuster oder Angriffsvektoren
- Ähnliche oder vergleichbare Maßnahmen zur Vermeidung und Risikominimierung

Dazu wurden in einem iterativen Arbeitsprozess Risikokategorien, Schritt 2 in Abbildung 9 formuliert:

- Organisatorische Sicherheit
- Eskalation und Kommunikation
- Naturgefahren
- Netzwerktechnik
- Normen und Recht
- Human Factor
- Fernwirk-Leittechnik
- Design-Architektur
- Hard-Software
- Planung und Beschaffung
- Zugriffskontrolle und Krypto

Diese Kategorien wurden den Einzelrisiken zugeordnet. Anschließend wurde eine thematische Gruppierung vorgenommen und daraus ein oder mehrere Aggregationsrisiken formuliert. In einem weiteren Schritt wurde ein auf diese Weise formuliertes Aggregationsrisiko anhand der Risikobewertungskriterien neu bewertet.

Dies wurde analog der Bewertung der Einzelrisiken im best-case, most-likely, und worst-case vorgenommen.

Parallel dazu wurde ein Risikoeigner formuliert und Maßnahmen zur Risikominimierung als Vorschlag erarbeitet.

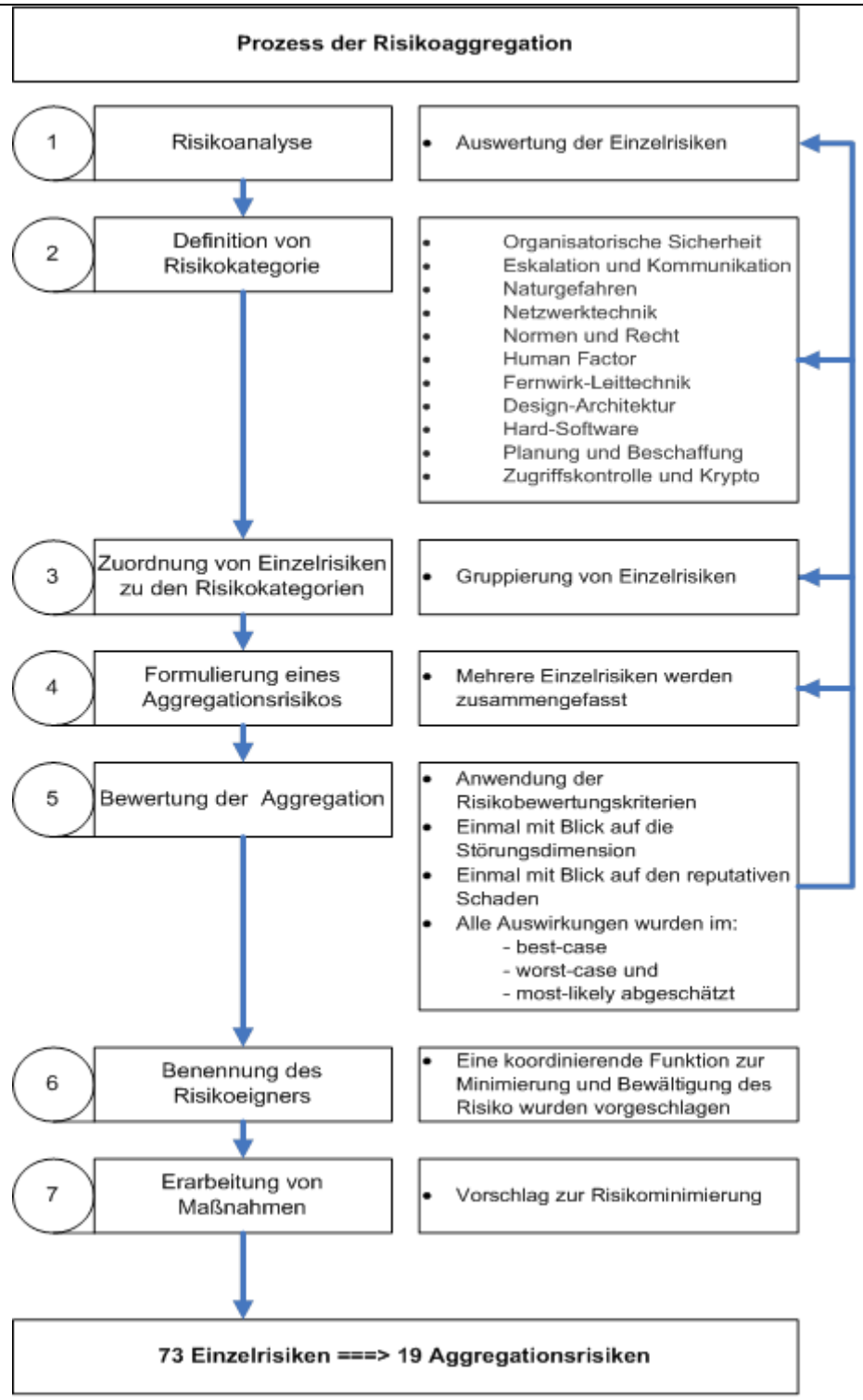


Abbildung 9: Risikoaggregationsprozess

11.2 Auswertung der Risikoverteilung nach Risikokategorien

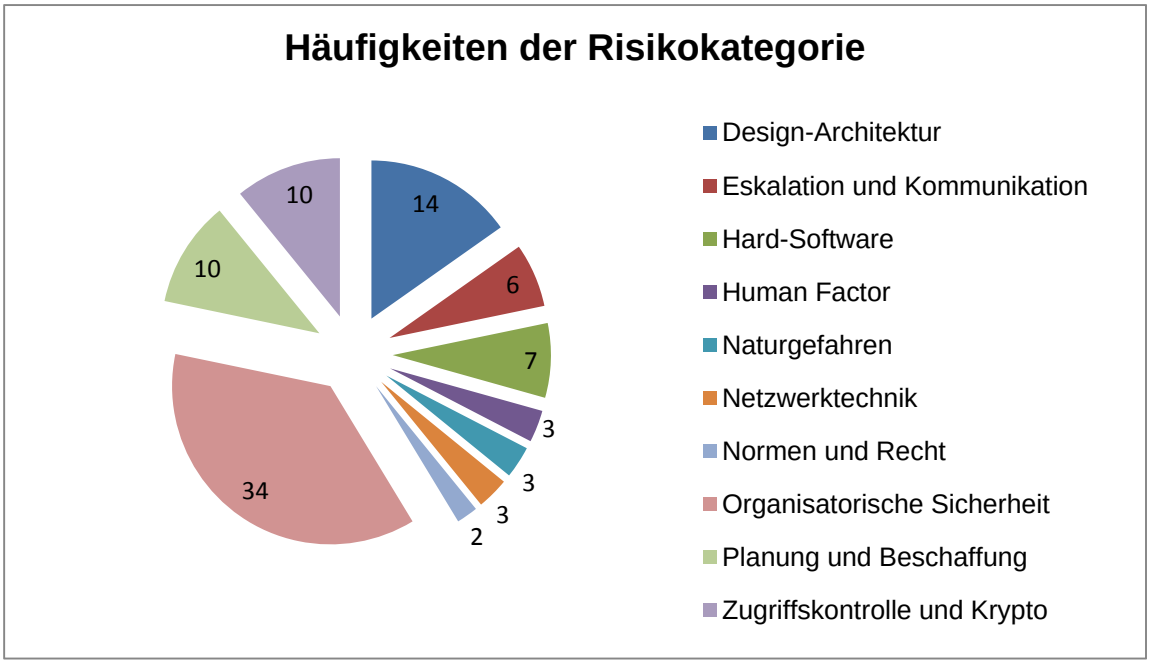


Abbildung 10: Verteilung der Risikokategorien

In Summe wurden 92 Risiken (73 Einzelrisiken + 19 Aggregationsrisiken) erfasst. In Abbildung 10 ist die relative Verteilung der Risiken in den gewählten Risikokategorien[18] dargestellt.

34 Risiken sind der „Organisatorischen Sicherheit zugeordnet“. Ein auf den ersten Blick augenscheinliches Ergebnis ist, dass die IKT-Risiken primär durch organisatorische Herausforderungen geprägt sind.

Dieses Bild zeigt einmal mehr, dass der Begriff „Sicherheit“ eine Konvergenz aus Safety und Security Herausforderungen ist. Sicherheit kann primär durch organisatorische Regelungen geschaffen, verbessert, beibehalten bzw. ausgebaut werden.

Sicherheit	
„Versorgungssicherheit“	
Safety	**Security**
Fahrlässigkeit ?, Schutz von Leib und Leben und materiellen Werten	Fahrlässigkeit, Intention, Vorsatz, Schutz von Leib und Leben, materiellen und immateriellen Werten

[18] Das Bild ist leicht verzerrt, da die Aggregationsrisiken zu den Einzelrisiken gleichwertig behandelt werden.

11.3 Maßnahmenzusammenfassung und -auswertung

Die Maßnahmenvorschläge wurden ausgewertet. Insgesamt wurden für die 19 Aggregationsrisiken 78 Maßnahmenvorschläge ausgearbeitet. Für die Erarbeitung von Empfehlungen wird folgende Gruppierung vorgeschlagen. Zusammenfassung von:

- Eskalation und Kommunikation
- Design und Architektur
- Human Factor
- Organisatorische Sicherheit
- Hard- und Software
- Normung und Recht
- Zugriffskontrolle und Kryptographie

Damit ergibt sich folgendes Bild (vgl. Abbildung 11):

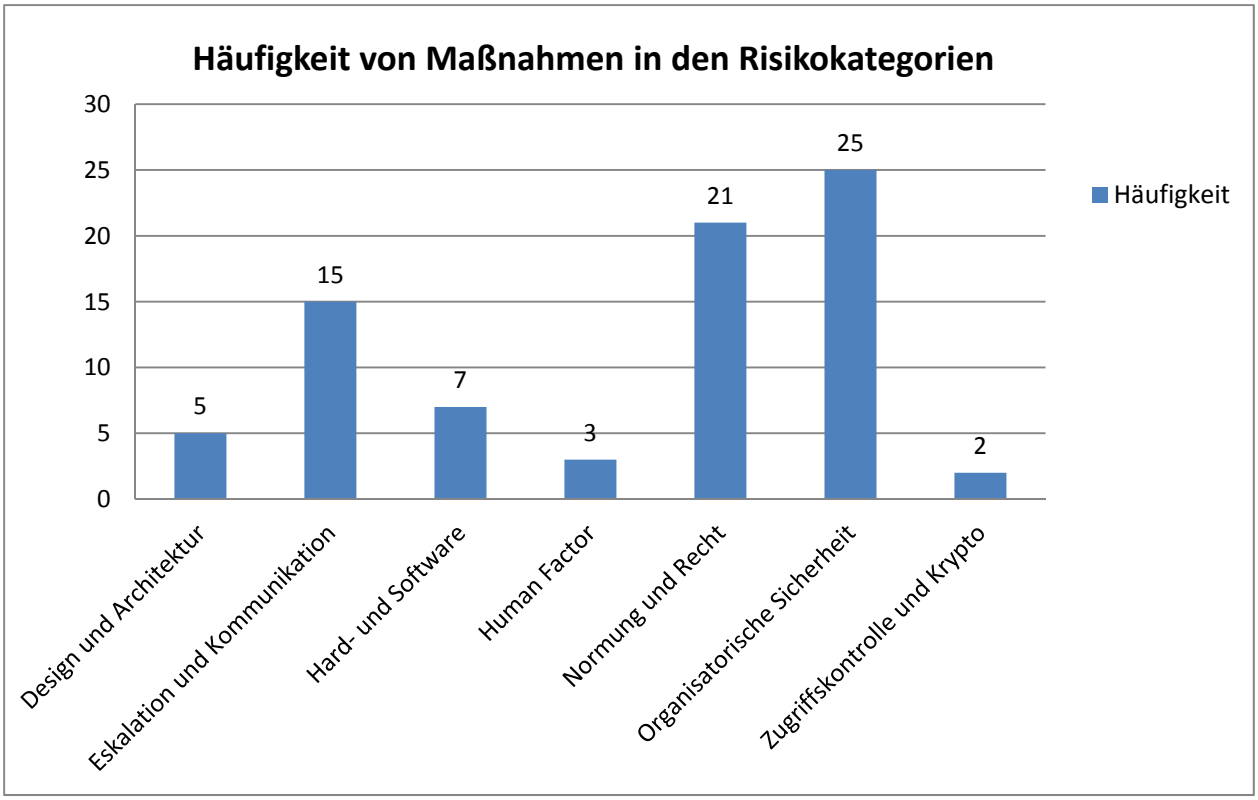


Abbildung 11: Verteilung der genannten Maßnahmen auf die Risikokategorien

Teil IV Empfehlungen

12 Maßnahmenaufstellung

Die Empfehlungen leiten sich aus den Maßnahmenvorschlägen ab. Die Maßnahmen zur Umsetzung werden für unterschiedliche Größen von Netzbetreibern und Erzeugern empfohlen, wobei die finale Definition zwischen großen und kleinen Netzbetreibern und Erzeugern in Abstimmung zwischen Öesterreichs Energie und dem APCIP-Prozess erfolgen muss.

In einem ersten Ansatz wird zwischen systemrelevanten Netzbetreibern und Erzeugern (Kurzbezeichnung „SysR“) und relevanten Erzeugern unterschieden (Kurzbezeichnung „Rel“).

Darüber hinaus werden drei Umsetzungsprioritäten definiert:

- Priorität 1 steht dabei für kurzfristig (vorrausichtlich bis 2 Jahre[19]),
- Priorität 2 steht dabei für mittelfristig (voraussichtlich 2-5 Jahre)
- Priorität 3 für eine langfristige Umsetzung (voraussichtlich >5 Jahre).

In einem hier angeregten Folgeprozess, der durch Öesterreichs Energie in Kooperation mit dem Projektlenkungsausschuss initiiert werden sollte, müssen die mit den erarbeiteten Maßnahmen verbundenen finanziellen und personellen Ressourcen identifiziert und abgestimmt werden. Dieser Prozess, legt:

- den Prozesseigner,
- die Prozessverantwortliche(n) und die Verantwortlichkeiten sowie
- die Umsetzungshorizonte fest.

Inwieweit die Empfehlungen für kleine Netzbetreiber und Erzeuger (z.B. Windparks) relevant sind, muss in einer gesonderten Signifikanzprüfung erfolgen.

Die von den Empfehlungen betroffenen rechtlichen Aspekte (z.B. Marktregeln und ELWOG) sind in Gleichklang mit den Umsetzungsergebnissen der ÖSCS-Arbeitsgruppen (Gruppe ordnungspolitischer Rahmen) zu bringen und in weiterer Folge durch den zuvor angesprochenen Folgeprozess zu prüfen.

[19] Beginn der Umsetzung

Teil V Anhänge

Übersicht der Anhänge

Anhang 1: Risikobewertungskriterien

Bewertungstabelle „Eintrittswahrscheinlichkeit

Technische Gefahren- und Naturgefahren				Machbarkeit Intentionale Gefahren		Bewertung Punkte
Eintritts-wahrscheinlichkeit	**Verbale Beschreibung**	**Mind. Häufigkeit 1 mal pro**		**Verbale Beschreibung**	**Aufwand in Zeit und Know-how**	
unwahrscheinlich	Das Ereignis bzw. die Gefahr ist unwahrscheinlich und tritt einmal in 50 Jahren auf.	50 Jahren		Sehr hoher Aufwand (auch finanziell) für die Tatausführung. Setzt Wissen voraus, das man sich durch sehr intensive Beschäftigung mit der Materie über einen längeren Zeitraum aneignen muss. Die Tat setzt auch voraus, dass man physische und organisatorische Barrieren unentdeckt überwinden kann.	Wochen - Monate der Vorbereitung/ Expertenniveau	**1**
selten	Das Ereignis bzw. die Gefahr ist selten und tritt langfristig einmal in 20 Jahren auf.	20 Jahren		Hoher Aufwand für die Tatausführung. Setzt Wissen voraus, das man sich durch intensive Beschäftigung mit der Materie aneignen kann. Die Tat setzt voraus, dass man physische und organisatorische Barrieren (auch soziale Kenntnisse) unentdeckt überwindet.	Wochen der Vorbereitung - spezielle Fachkenntnisse werden vorausgesetzt	**2**
gelegentlich	Das Ereignis bzw. die Gefahr ist denkbar und tritt mittelfristig einmal in 10 Jahren auf.	10 Jahren		Überschaubarer Aufwand für die Tatausführung. Das Ziel hat subjektiv eine gewisse Attraktivität. Die Tat setzt voraus, dass man physische Barrieren überwinden muss.	Tage der Vorbereitung- Fachkenntnisse werden vorausgesetzt	**3**
öfters	Das Ereignis bzw. die Gefahr ist möglich und tritt kurzfristig einmal in 1-5 Jahren auf.	5 Jahren		Geringer Aufwand für die Tatausführung. Das Ziel hat eine subjektiv hohe Attraktivität. Die Tat setzt voraus, dass IKT-basierte Barrieren überwunden werden müssen. Für die Tatausführung müssen jedoch eigene Werkzeuge geschaffen werden.	Wenige Tage der Vorbereitung werden vorausgesetzt.	**4**
häufig	Das Ereignis bzw. die Gefahr ist bekannt und tritt unterjährig auf.	Jahr oder öfter		Sehr geringer Aufwand für die Tatausführung. Das Ziel hat eine subjektiv hohe Attraktivität. Die Tat setzt voraus, dass IKT-basierte Barrieren überwunden werden müssen.	Es stehen bereits anpassbare Werkzeuge bzw. Werkzeugkisten zur Verfügung. Die Tat kann von interessierten Laien begangen werden.	**5**
				Aufwand wird auch finanziell verstanden		

Bewertungstabelle Auswirkungsdimension

Auswirkungen			
Auswirkung	**Verbale Beschreibung quantifizierend**	**Verbale Beschreibung qualitativ**	**Bewertung Punkte**
gering	Es sind mehr als 1 % der Anschlüsse im betrachteten Versorgungsgebiet von einer Stromunterbrechung für ca. 30 Min. betroffen. 1% der Peak Netz/Netz-Last des EVUs ist betroffen.	Versorgungsausfälle wie sie normalerweise auftreten können. Störung eines kleinen Teilnetzes (Abzweig) - kein reputativer Schaden	**1**
mittel	Es sind mehr als 2 % der Anschlüsse im betrachteten Versorgungsgebiet von einer Stromunterbrechung für ca. 1h betroffen. 2% der Peak Netz/Netz-Last des EVUs ist betroffen.	Ereignis bedingt organisatorisch-technischen Veränderungsbedarf in der IKT-Infrastruktur - geringer reputativer Schaden	**2**
hoch	Es sind mehr als 10 % der Anschlüsse im betrachteten Versorgungsgebiet von einer Stromunterbrechung für ca. 3h betroffen. 10% der Peak Netz/Netz-Last des EVUs ist betroffen.	Ereignis bedingt erheblichen organisatorisch-technischen Veränderungsbedarf in der IKT-Infrastruktur mit erheblichen personellen und finanziellen Ressourcen - reputativer Schaden, der nennenswerte finanzielle Ressourcen bindet um korrigiert zu werden	**3**
sehr hoch	Es sind mehr als 20 % der Anschlüsse im betrachteten Versorgungsgebiet von einer Stromunterbrechung für ca. 6h betroffen. 20% der Peak Netz/Netz-Last des EVUs ist betroffen.	Ereignis bedingt grundsätzliche organisatorisch-technische Veränderungen, da eine ausgenutzte Schwachstelle aufgrund der eingesetzten Hard- und Software nicht mittelbar geschlossen werden kann. Es existieren jedoch organisatorische Maßnahmen, welche die Schwachstellen überwachen und auswirkungsminimierende Maßnahmen können gesetzt werden. Sehr hoher reputativer Schaden	**4**
katastrophal	Es sind mehr als 50 % der Anschlüsse im betrachteten Versorgungsgebiet von einer Stromunterbrechung für ca. 12h betroffen, auch Totalausfall.	Ereignis bedingt grundsätzliche organisatorisch-technische Veränderungen, da eine ausgenutzte Schwachstelle aufgrund der eingesetzten Hard- und Software nicht mittelbar geschlossen werden kann. Katastrophaler reputativer Schaden	**5**
Für die Bewertung des „Schadens“ wird ein logisches „oder“ herangezogen und das für das EVU wichtigste Kriterium ausgewählt			

Anhang 2: Kurzbeschreibung der funktionalen Einheiten

NIST-AT Nr.	Beschreibung
1	Kraftwerksleittechnik, gesamte Betriebsführung auch z.B. Steuerung von Systemen der Gasturbine
2	Kunde
3	Kundengeräte
4	Erzeugung und Speicherung von Energie auf Kundenseite
5	Kunden Energiemanagement System
6	Elektrische Fahrzeuge
7	Schnittstelle Energielieferanten zu Kunde/Kundennetzwerk (HAN-Gateway)
8	Zähler
9	Anzeige, ist keine lokale Schnittstelle sondern ein "Homedisplay", kann proprietär sein
10	ist für künftige Analysen reserviert
11	Wasser und Gaszähler. Trennung von Zählern und Schnittstelle zwischen Zählern, es gibt derzeit keine Mehrspartenzähler aber die Zähler können miteinander kommunizieren
12	Datenkonzentrator. Könnte ein Zähler sein, der auch Gas/Wasser/Wärmewert mit aufzeichnet oder WiMax-Station an/im Trafo, der Werte an MDM sendet.
13	Kann eine intelligente Ortsleitstation sein, oder auch ein intelligenter Zähler
14	Distribution Automation Field Devices. Multifeatured installations meeting a broad range of control, operations, measurements for planning, and system performance reports for the utility personnel.
15	RTU/IED-Sensor Remote Terminal Unit entspricht 46 und 47 in einem
16	Außendienstwerkzeuge, primär für Maintenance Zwecke
17	GIS oder NIS Systeme
18	Sensoren aller Art, auch Umweltsensoren
19	ist für künftige Analysen reserviert
20	Stromhändler. Eine natürliche oder juristische Person oder Erwerbsgesellschaft, die Elektrizität in Gewinnabsicht verkauft
21	Headend-Frontendrechner für SMART Meter
22	Großspeichersysteme auch Speicherkraftwerke
23	Kundeninformationssysteme nicht CRM
24	Servicemitarbeiter
25	Steuerungssystem für ein virtuelles Kraftwerk, (für künftige Smart-Grid-Applikationen reserviert, fraglich ob es so etwas bei 2020 geben wird) -Auch bei Windkraftwerken
26	Netzplanung
27	Verteilungsmanagementsystem
28	Verteilungssystem-Operator "eine Person"
29	Verteilung-SCADA

NIST-AT Nr.	Beschreibung
30	Energie Management System. Höherwertige Funktionen als bei einem SCADA System.
31	Leitzentrale für großflächiges Lastmanagement und Netzsicherheit. Entspricht der APG
32	Analoge Funktion zu 5 (Kunden Energie Managementsystem)
33	MDMS Meter Data Management System MDM
34	Zähler/Verrechnungs-Backofficedienst z.B. Weboberfläche zum Billing auf MDM - ist derzeit in Österreich vermutlich nicht installiert, existiert aber
35	ist für künftige Analysen reserviert
36	OMS Outage Management System
37	Übertragungs-SCADA
38	Kundenportal
39	Wide Area Messsysteme für Lagebeurteilungen. Nr. 45 und 39 sind häufig miteinander kombiniert.
40	Work Management (Workforce) Management
41	Stromlieferant -Vertrieb
42	Prozess der Verrechnung
43	Energiedienstleister
44	Dritte / Fremdsysteme
45	PQ Messeinheit elektrischer Parameter Phasor Measurement Unit: APG hat so etwas im Einsatz, = Power Quality (PQ) auch PMU
46	Intelligente, elektronische Übertragungsgeräte auch "Schutzgerät", aber zusätzlich mit Veränderung des Spannungslevels (Trafo)
47	Fernwirkgerät (Datenübertragung SCADA zu/von Feldsystemen) bei APG sind 47 und 15 zum Teil gleich
48	ist für künftige Analysen reserviert
49	Primärtechnik
50	Schnittstelle zu ECA z.B. Meldepflichten
51	ist für künftige Analysen reserviert
52	BKO, Bilanzgruppenkoordinator Eine natürliche oder juristische Person, die eine Verrechnungsstelle für die Organisation und die Abrechnung der Ausgleichsenergieversorgung innerhalb einer Regelzone aufgrund einer behördlichen Konzession betreibt;
53	BGV Eine gegenüber anderen Marktteilnehmern und dem Bilanzgruppenkoordinator zuständige Stelle einer Bilanzgruppe, welche die Bilanzgruppe vertritt.
54	NB Netzbetreiber
55	Regelzonenführer
56	Engpassmanagement
57	Telekomprovider intern oder extern überträgt Daten

Anhang 3: Gefahrenkatalog gesamt

Nr.	Gefahrenbeschreibung
1	Gefahr einer absichtlichen, aber nicht autorisierten Auslösung von Schalthandlungen, die keine User Identifizierung oder Authentifizierung benötigen
2	Gefahr, dass Unbefugte Zugang zu nicht privilegierten Remote-Access-Accounts, LAN-Accounts mit Privilegien oder Remote- Access- LAN- Accounts mit Privilegien erhalten
3	Gefahr, dass Maschinen/Equipment ohne organisatorische eineindeutige Identifikation im LAN/Netzwerk/Fernwirksystem/Netzleitsystem/Prozessleitsystem in Betrieb genommen werden können (Organisatorisch - MAC, oder Maschinenzertifikate)
4	Gefahr, dass während der Authentifizierung Authentifizierungsinformationen an unbefugte Dritte zurückgegeben werden (Bsp. Maskieren der Passwortinformationen)
5	Gefahr, dass im abgeschotteten LAN/Netzwerk/Fernwirksystem/Netzleitsystem/Prozessleitsystem DDoS-Angriffe durchgeführt werden können
6	Gefahr, dass konzeptionelle Schwachstellen bei der Trennung von LAN/Netzwerk/Fernwirksystem/Netzleitsystem/Prozessleitsystem zu anderen LAN/Netzwerk/Fernwirksystem/Netzleitsystem/Prozessleitsystem übersehen wurden
7	Gefahr, dass die Integrität eingeführter und abgesicherter Kommunikation kompromittiert wird
8	Gefahr, dass die Vertraulichkeit eingeführter und abgesicherter Kommunikation kompromittiert wird
9	Gefahr, dass ungeprüfte Software/Firmware/Code im produktiven Betrieb eingesetzt wird und damit die funktionale Sicherheit oder security-relevante Funktionen "gestört" werden können
10	Gefahr, dass eine (konzeptionelle) Schwäche in der funktionalen Sicherheit ein vorgesehenes Security-Features kompromittiert
11	Gefahr, dass durch eine zunehmende Heterogenität in der IKT-Sicherheitsarchitektur ausnutzbare Schwachstellen, die zur Manipulation mit Schadwirkung ausnutzbar sind, zu spät erkannt werden
12	Gefahr, dass das Key-Management aus organisatorischen Defiziten heraus mangelhaft implementiert ist und sich daraus zusätzliche funktionale Sicherheitsschwächen und/oder Securitylücken ergeben, die für Schadwirkungen ausnutzbar sind
13	Gefahr der vorsätzlichen physischen Trennung von Datenleitungen und Nachrichtenübertragung durch intentionale Gefahren
14	Gefahr von technischen Defekten bei Übertragungs- und Netzwerktechnik (z.B. Netzwerkkomponenten wie Switches, Router Konzentratoren) oder Sicherheitseinrichtungen
15	Gefahr, dass aufgrund von nicht klar geregelten Haftungsfragen, technische Innovationen, die der Sicherheit dienen, nicht eingeführt werden
16	Elementarereignisse (Hochwasser, Starkniederschläge, **Feuer, etc.)**
17	Ausfall oder Störung von Kommunikationsnetzen
18	Gefahr, dass aufgrund von Regulatorvorgaben (auch finanzielle Rahmenbedingungen), technische Innovationen, die der Sicherheit dienen, nicht eingeführt werden
19	Gefahr von elektromagnetischer Störstrahlung (EMP)
20	Gefahr von Software-Schwachstellen oder -Fehlern

Nr.	Gefahrenbeschreibung
21	Gefahr der Manipulation von Hard- oder Software
22	Gefahr der Offenlegung schützenswerter Informationen
23	Unzureichende Security und Safetyfestlegung in den Fernwirkprotokollen der Energieversorger IEC60870-5 Profil 101-104, und IEC 60870-6, TASE 2 (ICCP), IEC61850 die bis dato fehlende Erfahrung im Umgang mit den Zertifikaten und Ablauf bei den Zertifikaten ==> Ausfall der Kommunikation Es gibt derzeit noch keine Systemlösungen, Implementierung und die Ausrollphase
24	Gefahr von nicht erkannten Safety und Security-Schwachstellen und der lange Nutzungszeitraum
25	Gefahr, dass **geprüfte** Software einen erheblichen funktionalen Fehler aufweist
26	Gefahr, dass die Performance der Endgeräte zu gering ist (Kommunikationsbandbreite und Rechenkapazität) auch eine langfristige Perspektive
27	Gefahr, dass Auslegungskriterien zu konservativ beurteilt werden (Planungsfehler!)
28	Gefahr der reaktiven Instandhaltungsphilosophie
29	Gefahr, dass Änderungen von Strukturen und Designs keinen **regelmäßigen** hollistischen Betrachtungen unterzogen werden
30	Gefahr, dass mit Endgeräten ohne Spannungsversorgung, USV und Pufferung keine Kommunikation (bei Ausfall von Strom) mehr möglich ist (zeitlich ab > = 8h)
31	Gefahr, dass das Securitykonzept keine rechtzeitigen Gegenmaßnahmen erlaubt
32	Gefahr, dass durch Manipulation an Zeitgebern die M2M -Kommunikation erheblich gestört wird (Funkuhr und GPS-Manipulation)
33	Gefahr ungenügender Prüfroutinen auf umfassende funktionale Sicherheit
34	Gefahr, dass die Software zu wenig defensiv programmiert wurde
35	Gefahr der fehlenden Awareness im Umgang mit alten Betriebssystemen und bei Security Themen (intern und extern, auch Lieferanten)
36	Gefahr von fehlender Long-Term-Support von Wartungssoftware und OS und DBs
37	Gefahr der fehlenden Erfahrung/Schulung im Umgang mit Wartungssoftware
38	Gefahr des unzureichenden Umgangs bei "near miss" Zuständen (Safurity) ===> CIRS
39	Gefahr Ausfall des OSI-Layers 1-3 (Ursache Technik, auch Software, Naturgefahr, Intentionale)
40	Gefahr der heterogenen IKT-Landschaft - Seiteneffekte wenig bekannt
41	Gefahr der fehlenden Technologiefolgenabschätzungen
42	Gefahr, dass zentrale Services der RTU-Infrastruktur kompromittiert/gestört werden
43	Gefahr der fehlende Awareness der Hersteller für IT-Sec bei Fernwirk- und Netzleittechnik ===> (Aufwand/Kosten bei den Herstellern) besser Kollaboration und Kommunikation bei den Betreibern
44	Hochwasser- Unterbrechung von bodengebundenen Kommunikationskanälen (Unterbrechung von Kommunikation)
45	Starkniederschlagereignisse- Unterbrechung der Kommunikation
46	Gefahr, dass durch Kaskaden mehrerer untergeordneter Kommunikationsprozesse ein kritischer Prozess gestört wird (In der Wirkung ähnlich einem DDoS oder aber auch nicht beabsichtigen Shut-Down)
47	Gefahr eines unautorisierten Zugriffs über das Netzwerk auf IKT-Einrichtungen mit der Möglichkeit, gezielte oder ungezielte Schalthandlungen durchzuführen

Nr.	Gefahrenbeschreibung
48	Gefahr eines unautorisierten Zugriffs über das Netzwerk auf IKT-Einrichtungen mit der Möglichkeit, Daten auszuspionieren und/oder zu veröffentlichen
49	Gefahr eines unautorisierten Zugriffs über das Netzwerk auf IKT-Einrichtungen mit der falsche Daten an Bediener/System vorzutäuschen
50	Elementarereignisse (Hochwasser, fehlendes Kühlwasser, Starkniederschläge etc.) G.05 BSI
51	Gefahr des Ressourcenmangels
52	Gefahr mangelnder Objektschutz
53	Gefahr der mangelhaften Organisation des Wechsels zwischen den Benutzern
54	Gefahr durch fehlende oder unzureichende Dokumentation
55	Gefahr unkoordinierter Schalthandlungen Kraftwerk-Netz
56	Gefahr von unvorhergesehenen Kaskadeneffekten innerhalb einer Organisation, die zu einem Stromausfall führen können
57	Gefahr von nicht erkannten Serienfehlern ==> schlimmer bei homogener Infrastruktur
58	Gefahr logischer Fehler von redundanten gleichen Systemen
59	Gefahr von Hochwasser, Unterbrechung von bodengebundenen Kommunikationskanälen (Unterbrechung von Kommunikation)
60	Gefahr von Starkniederschlagereignissen und dadurch bedingter Unterbrechung der Kommunikation
61	Gefahr, dass Sicherheitsrichtlinien wie z.B. Bildschirmsperrung nach einer definierten Zeit usw. umgangen werden bzw. nicht implementiert sind
62	Gefahr einer absichtlichen, aber nicht autorisierten Auslösung von Aktionen, die keine User Identifizierung oder Authentifizierung benötigen
63	Gefahr, dass die eingesetzten kryptographischen Verfahren und Prozesse den Schutz der Daten nicht mehr sicherstellen können oder sonst irgendwie umgangen werden können
64	Gefahr, dass durch Kaskaden mehrerer untergeordneter Kommunikationsprozesse ein kritischer Prozess gestört bzw. ausgelöst wird (in der Wirkung ähnlich einem DDoS oder aber auch nicht beabsichtiger Shut-Down)
65	Gefahr eines unautorisierter Zugriffs über das Netzwerk auf IKT-Einrichtungen mit der Möglichkeit, gezielte oder ungezielte Manipulation durchzuführen
66	Gefahr, dass absichtliche Manipulationen an Backoffice-Systemen mit einer Schadwirkung auf einen anderen Netzbetreiber nicht rechtzeitig erkannt werden
67	Gefahr, dass malicous Code den Ausfall von Smart-Metern, Transaktionsservern oder Backoffice Systemen zur Folge hat
68	Gefahr der Einschleppung eines Virus
69	Gefahr der Einschleppung eines Trojaners
70	Gefahr der Verletzung von Datenschutzvorgaben (MDM-Headend-Zähler)
71	Gefahr der Verletzung von Datenschutzvorgaben (Office-Umfeld)
72	Gefahr der vorsätzlichen Abschaltung durch den Backoffice-Prozess bei x-tausend Kunden
73	Gefahr von technischer Fehlern in/bei Hard/Softwarekomponenten, die ein (Broadcast) an x-tausend Kunden verursachen kann
74	Gefahr eines menschl. Versagens, das die Abschaltung von x- tausend Kunden zur Folge hat
75	Gefahr von Fehlern im Rollenkonzept im Office/Backofficeprozess == > unkontrollierte Aktivierung
76	Gefahr der Verwundbarkeit von Kundeninformationssystemen mit einer möglichen Schnittstelle zum MDM ====> Empfehlungen entsprechendes Zonenkonzept erarbeiten und umsetzen und regelmäßig überprüfen lassen

Nr.	Gefahrenbeschreibung
77	Gefahr, dass Instrumente des Workforce Management (Inhalte) in kriminelle Hände gelangen z.B. mögliche Schalthandlungen auslösen ?.... === > Awareness und Schulungsthema
78	Gefahr, dass im WAN/LAN/Netzwerk/Fernwirksystem/Netzleitsystem/Prozessleitsystem DDoS-Angriffe durchgeführt werden können
79	Gefahr, dass die Integrität eingeführter und abgesicherter Kommunikation kompromittiert wird (Fahrplanmanagement)
80	Gefahr, dass die Vertraulichkeit eingeführter und abgesicherter Kommunikation kompromittiert wird (Fahrplanmanagement)
81	Gefahr des Ausfalls von Internetkommunikation zwischen den Marktteilnehmers >= 12h Ersatzkommunikation für das Fahrplanmanagement vorsehen
82	Gefahr einer DDoS-Attacke auf die Internet-/Intranetkommunikation bei EVUs
83	Gefahr einer DNS-Manipulation der Internet-/Intranetkommunikation bei EVUs
84	Gefahr, dass Trojaner die Fahrpläne kompromittieren
85	Gefahr von Softwarefehlern im Fahrplanmanagement bei APCS und APG
86	Gefahr eines Angriffs auf das Fahrplanmanagement bei APCS und APG durch einen gezielten Angriff
87	Technische Defekte bei Übertragungs- und Netzwerktechnik (z.B. Netzwerkkomponenten wie Switches, Router Konzentratoren) oder Sicherheitseinrichtungen
88	Gefahr, dass Fehlerstromsensor umgangen werden
89	Gefahr, dass Case-Openingsensoren umgangen werden
90	Gefahr, Passwort reset attempts zum Erfolg führen
91	Gefahr, dass eine automatisierte Regelung von Stellgrößen von Daten aus den Smart Metern bei den Trafostationen (örtlich disloziert bei den derzeitigen Konzentratoren) versagt
92	Gefahr, dass eine automatisierte Regelung von Stellgrößen von Daten aus den Smart Metern bei den Trafostationen (örtlich disloziert bei den derzeitigen Konzentratoren) manipuliert werden kann
93	Gefahr des flächendeckenden Ausfalls einer kritischen Komponente im Smart Meter mit unmittelbarer Rückwirkung auf eine künftige Smart Grid Applikation
94	Gefahr des Ansteigens von Echtzeitregelbedarf im Niederspannungsbereich durch volatile und dezentrale Energieeinspeisung mit möglicher negativer Auswirkung auf die Versorgungssicherheit
95	Gefahr, dass absichtliche Manipulationen an "MDMS-Systemen" mit einer Schadwirkung auf einen anderen Netzbetreiber oder aber auch auf die eigene Organisation nicht rechtzeitig erkannt werden
96	Gefahr, dass im WAN/LAN/Netzwerk/Fernwirksystem/Netzleitsystem/Prozessleitsystem DDoS-Angriffe durchgeführt werden können (NB Bei Großkunden)
97	Gefahr, dass über das Internet HAN-fähige Verbraucher gleichzeitig eingeschaltet werden, ausgelöst z.B. durch ein Botnetz
98	Session Lock, Gefahr von nicht beendeten Sessions bzw. unkoordinierten und "unüberwachten" Sessions, die von einem Unbefugten für Manipulationen ausgenutzt werden können
99	Remote Session Termination, Gefahr von unkoordinierten Remote Sessions, die von einem Unbefugten für Manipulationen ausgenutzt werden können
100	Remote Access -Control, Gefahr des unbefugten, unberechtigten oder unkontrollierten befugten Zugriffs mit einer möglichen Schadwirkung
101	Gefahr, dass Normen für die Entwicklung sicherer Software nur bedingt eingesetzt werden (z.B. V-Modelle, IEC 61508 ff)

Nr.	Gefahrenbeschreibung
102	Konfigurationsfehler, Fehlinstallationen und/oder Wartungsfehler
103	Gefahr, dass Service und Wartungsgeräte (PDA, Laptops etc) durch unbefugte externe Dritte in Besitz genommen werden und darauf unbemerkt Manipulationen über einen längeren Zeitraum (Wochen - Monate) vornehmen können
104	Gefahr, dass unzureichende Spezifikationen bei der Beschaffung von Komponenten keine für den Betrieb ausreichende funktionale Sicherheit und/oder Security sicherstellen
105	Objektschutz Netzstation
106	Physischer Schutz kritischer IKT-Einrichtungen
107	Menschl. Fehler /Fehlbedienungen
108	Social Engineering
109	Fehlende Notfallplanung und Eskalationskultur im BCM
110	Zutritt Trafostation
111	Mängel in /bei Sicherheitsüberprüfungen, Freigabeprozessen und Darstellung der erreichten Security
112	Mängel bei Beweisbarkeit Nachvollziehbarkeit von "Schadaktionen"
113	Breiter Stromausfall über längeren Zeitraum
114	Verzögerte oder keine Reaktion auf Vorfälle

Anhang 4: Übersicht von Gesetzen, Normen und Richtlinien

Legende:

RM: primär dem Risikomanagement und Sicherheitsmanagement zugeordnet

SM, NM, KM: dem Störungs-, Notfall-, und Krisenmanagement zugeordnet

Gesetz, VO, Norm, Regelung	Kurzbeschreibung	RM	SM,NM, KM
GESETZE:			
Aktiengesetz	§81 Bericht an den Aufsichtsrat, §82 Rechnungswesen, § 84 und § 92 Sorgfaltspflicht und Verantwortlichkeit der Vorstandsmitglieder bzw. Aufsichtsräte	x	x
AngG § 18	Fürsorgepflichten		x
Arbeitszeitruhegesetz	Überschreitung der Ruhezeiten	x	x
ASchG	Arbeitsunfälle	x	x
Bauarbeiten-koordinationsgesetz	Sicherheits- und Gesundheitsschutzplan gem. §7 Abs. 1	x	x
Datenschutzgesetz DSG	Bundesgesetz über den Schutz personenbezogener Daten	x	x
E-Government-Gesetz - E-GovG	Bundesgesetz über Regelungen zur Erleichterung des elektronischen Verkehrs mit öffentlichen Stellen		x
ELWOG, GWG	Landes ELWOGs beachten „Branchenspezifische Regelungen“	x	x
Energieversorgungssicherheitssgesetz			x
Feuerpolizeigesetz	Präventive Maßnahmen	x	x
Gesundheitstelematikgesetz-GTelG	Bundesgesetz betreffendDatensicherheitsmaßnahmenbeim elektronischen Verkehr mitGesundheitsdaten und Einrichtung einesInformationsmanagement	x	x

Gesetz, VO, Norm, Regelung	Kurzbeschreibung	RM	SM,NM, KM
Gewerbeordnung	§84, bzw. §84c Pflichten des Betriebsinhabers, Abschnitt 8a Sicherheitsbericht etc	x	x
GmbH Recht	§ 25 Abs. 1, §28 Sorgfaltspflicht des GF, Aufbau internes Kontrollsystem	x	x
Informationssicherheitsgesetz InfoSiG	Verpflichtungen zur sicheren Verwendung von Informationen	x	
Katastrophenschutzgesetze der Länder	Katastrophenschutz	x	x
Konsumentenschutzrecht	Verträge und Vereinbarungen mit Konsumenten	x	x
Medienrecht	Öffentlichkeitsarbeit, Veröffentlichungen etc.		x
RLÄG	Vgl. §267 Abs.1 UGB und §243 UGB	x	
Schadensersatzrecht	Dokumentationspflicht	x	x
Sicherheitspolizeigesetz SPG	Bundesgesetz über die Organisation der Sicherheitsverwaltung und die Ausübung der Sicherheitspolizei		x
Signaturgesetz - SigG	Bundesgesetz über elektronische Signaturen	x	
Strafgesetzbuch StGB	Vergehen bzw. Verbrechenstatbestände	x	x
Strafprozessordnung StPO	i.V. mit Vergehen und Verbrechen n. d. StGB		x
Telekommunikationsgesetz	Stammfassung: BGBl. I Nr. 100/1997	x	x
UGB,Unternehmens-gesetzbuch	Bundesgesetz über besondere zivilrechtliche Vorschriften für Unternehmen	x	x
URÄG	§237 Abs. 8a, §266 Z 2a UGB	x	
Urheberrechtsgesetz	Bundesgesetz über das Urheberrecht an Werken der Literatur und der Kunst und über verwandte Schutzrechte	x	x
Verbandsverantwortlichkeits-gesetz	Im wesentlichen Sorgfaltspflichten, legt auch Sanktionen fest ebenda §3	x	

Gesetz, VO, Norm, Regelung	Kurzbeschreibung	RM	SM,NM, KM
VERORDNUNGEN:			
Informationssicherheits-verordnung InfoSiV	Verordnung der Bundesregierung über die Informationssicherheit	x	
HalonbankV	Verordnung über die Einrichtung einer Halonbank (Halonbankverordnung - HalonbankV), BGBl. II Nr. 77/2000	x	
Halonverbot	Verordnung über das Verbot von Halonen, BGBl. Nr. 576/1990	x	
SigV	Verordnung des Bundeskanzlers über elektronische Signaturen (Signaturverordnung 2008 - SigV), Stammfassung: BGBl. II Nr. 3/2008	x	
V A-SIT	Verordnung des Bundeskanzlers über die Feststellung der Eignung des Vereins "Zentrum für sichere Informationstechnologie - Austria (ASIT)" als Bestätigungsstelle, BGBl. II Nr. 31/2000	x	
StMV	Standard- und Muster-Verordnung 2004 (StMV 2004), Stammfassung: BGBl II Nr. 312/2004	x	
ESV 2003	Elektroschutzverordnung 2003	x	x
SVP-VO	Verordnung über die Sicherheitsvertrauenspersonen		x
BS-V	Bildschirmarbeitsverordnung	x	
AStV	Arbeitsstättenverordnung	x	x
AM-VO	Arbeitsmittelverordnung	x	x
GKV	Grenzwerteverordnung	x	x
FK-V	Fachkenntnisnachweis-Verordnung	x	x

Gesetz, VO, Norm, Regelung	Kurzbeschreibung	RM	SM,NM, KM
VGÜ	Verordnung über die Gesundheitsüberwachung am Arbeitsplatz	x	x
ARG-VO	Arbeitsruhegesetz-Verordnung	x	x
KGVo	Kontrollgeräte-Verordnung	x	x
NORMEN:			
IEC 80001-1:2010	Application of risk management for IT-Networks incorporating medical devices -- Part 1: Roles, responsibilities and activities	x	
ISO 31000	Risikomanagement	x	
ISO 9001	Qualitätsmanagement	x	
ISO NORMEN 11568-2:2005	Banking - Key management (retail) - Part 2: Symmetric ciphers, their key management and life cycle	X	
ISO NORMEN 11568-4:2007	Banking - Key management (retail) - Part 4: Asymmetric cryptosystems - Key management and life cycle	X	
ISO NORMEN 13491-1:2007	Banking - Secure Cryptographic devices (retail) - Part 1: Concepts, requirements and evaluation methods	X	
ISO NORMEN 13491-2:2005	Banking - Secure Cryptographic devices (retail) - Part 2: Security compliance checklists for devices used in financial transactions	X	
ISO NORMEN 13492:2007	Financial services - Key management related data element - Application and usage of ISO 8583 data elements 53 and 96	X	
ISO NORMEN 15892:2000	Space data and information transfer systems - Protocol specification for space communications - Security protocol	X	

Gesetz, VO, Norm, Regelung	Kurzbeschreibung	RM	SM,NM, KM
ISO NORMEN 19092:2008	Financial services -- Biometrics -- Security framework	X	
ISO -NORMEN 22857:2004	Health informatics - Guidelines on data protection to facilitate trans-border flows of personal health information	X	
ISO NORMEN TR 13569:2005	Financial services - Information security guidelines	X	
ISO NORMEN TR 14742:2010	Financial services - Recommendations on cryptographic algorithms and their use	X	
ISO NORMEN TS 13606-4:2008	Health informatics - Electronic health record communication - Part 4: Security	X	
ISO NORMEN TS 21547:2010	Health informatics -- Securityrequirements for archiving of electronichealth records -- Principles	X	
ISO NORMEN TS 24534-4:2010	Automatic vehicle and equipment identification - Electronic Registration Identification (ERI) for vehicles - Part 4: Secure communications using asymmetrical techniques	X	
ISO NORMEN TS 24534-5:2008	Automatic vehicle and equipment identification - Electronic Registration Identification (ERI) for vehicles - Part 5: Secure communications using symmetrical techniques	X	
ISO PAS 28000 Serien (ISO PAS 28001 und ISO PAS 28004):	Rahmenwerk zur Sicherheit der Lieferkette	X	
ISO und IEC-NORMEN 10116:2006	Information technology - Modes of operation for an n-bit block cipher	X	
ISO und IEC-NORMEN 10118-1:2000	Information technology- Security techniques - Hash functions - Part 1: General	X	

Gesetz, VO, Norm, Regelung	Kurzbeschreibung	RM	SM,NM, KM
ISO und IEC-NORMEN 10118-2:2010	Information technology- Security techniques - Hash functions - Part 2: Hash-functions using an n-bit block cipher	X	
ISO und IEC-NORMEN 10118-3:2004	Information technology- Security techniques - Hash functions - Part 3: Dedicated hash-functions	X	
ISO und IEC-NORMEN 10118-4:1998	Information technology- Security techniques - Hash functions - Part 4: Hash-functions using modular arithmetic	X	
ISO und IEC-NORMEN 10164-7:1992	Information technology - Open Systems Interconnection - Systems Management: Security alarm reporting function	X	
ISO und IEC-NORMEN 10164-8:1993	Information technology - Open Systems Interconnection - Systems Management: Security audit trail function	X	
ISO und IEC-NORMEN 10181-Parts 1-7:1996	Information technology - Open systems interconnection - Security frameworks for open systems	X	
ISO und IEC-NORMEN 10736:1995	Information technology - Telecommunications and information exchange between systems - Transport layer security protocol	X	
ISO und IEC-NORMEN 10745:1995	Information technology - Open Systems Interconnection - Upper layers security model	X	
ISO und IEC-NORMEN 11577:1995	Information technology - Open Systems Interconnection - Network layer security protocol	X	
ISO und IEC-NORMEN 11586-Parts1-6:1996	Information technology - Open Systems Interconnection - Generic upper layers security	X	

Gesetz, VO, Norm, Regelung	Kurzbeschreibung	RM	SM,NM, KM
ISO und IEC-NORMEN 11770-1:1996	Information technology - SecurityTechniques - Key Management - Part 1:Framework	X	
ISO und IEC-NORMEN 11770-2:2008	Information technology - Security Techniques - Key Management - Part 2: Mechanisms using symmetric techniques	X	
ISO und IEC-NORMEN 11770-3:2008	Information technology - Security Techniques - Key Management - Part 3: Mechanisms using asymmetric techniques	X	
ISO und IEC-NORMEN 11770-4:2006	Information technology - Security Techniques - Key Management - Part 4: Mechanisms based on weak secrets	X	
ISO und IEC-NORMEN 13157-1:2010	Information technology - Telecommunications and information exchange between systems - NFC Security - Part 1: NFC-SEC NFCIP-1 security services and protocol	X	
ISO und IEC-NORMEN 13157-2:2010	Information technology - Telecommunications and information exchange between systems - NFC Security - Part 2: NFC-SEC cryptography standard using ECDH and AES	X	
ISO und IEC-NORMEN 13888-1:2009	Information technology - Security techniques - Non-repudiation - Part 1: General	X	
ISO und IEC-NORMEN 13888-2:1998	Information technology - Security techniques - Non-repudiation - Part 2: Mechanisms using symmetric techniques	X	
ISO und IEC-NORMEN 13888-3:2009	Information technology - Security techniques - Non-repudiation - Part 3: Mechanisms using asymmetric techniques	X	

Gesetz, VO, Norm, Regelung	Kurzbeschreibung	RM	SM,NM, KM
ISO und IEC-NORMEN 14888-1:2008	Information technology - Security techniques - Digital signatures with appendix - Part 1: General	X	
ISO und IEC-NORMEN 14888-2:2008	Information technology - Security techniques - Digital signatures with appendix - Part 2: Integer factorization based mechanisms	X	
ISO und IEC-NORMEN 14888-3:2006	Information technology - Security techniques - Digital signatures with appendix - Part 3: Discrete logarithm based mechanisms	X	
ISO und IEC-NORMEN 15292:2001	Information technology - Security techniques - Protection Profile registration procedures	X	
ISO und IEC-NORMEN 15408-1:2009	Information technology- Security techniques- Evaluation criteria for IT security - Part 1: Introduction and general model	X	
ISO und IEC-NORMEN 15408-2:2008	Information technology- Securitytechniques- Evaluation criteria for ITsecurity - Part 2: Security functionalcomponents	X	
ISO und IEC-NORMEN 15408-3:2008	Information technology- Security techniques- Evaluation criteria for IT security - Part 3: Security assurance components	X	
ISO und IEC-NORMEN 15446:2009	Information technology - Security techniques - Guide for the production of Protection Profiles and Security Targets	X	
ISO und IEC-NORMEN 15816:2002	Information technology - Security techniques - Security information objects for access control	X	

Gesetz, VO, Norm, Regelung	Kurzbeschreibung	RM	SM,NM, KM
ISO und IEC-NORMEN 15945:2002	Information technology - Security techniques - Specification of TTP services to support the application of digital signatures	X	
ISO und IEC-NORMEN 15946-1:2008	Information technology - Security techniques - Cryptographic techniques based on elliptic curves - Part 1: General	X	
ISO und IEC-NORMEN 15946-5:2009	Information technology - Security techniques - Cryptographic techniques based on elliptic curves - Part 5: Elliptic curve generation	X	
ISO und IEC-NORMEN 16500-7:1999	Information technology -- Generic digital audio-visual systems -- Part 7: Basic security tools	X	
ISO und IEC-NORMEN 18014-1:2008	Information technology - Security techniques - Time stamping services -- Part 1: Framework	X	x
ISO und IEC-NORMEN 18014-2:2009	Information technology - Security techniques - Time stamping services - Part 2: Mechanisms producing independent tokens	X	
ISO und IEC-NORMEN 18014-3:2009	Information technology - Security techniques - Time stamping services - Part 3: Mechanisms producing linked tokens	X	
ISO und IEC-NORMEN 18028-2:2006	Information technology - Security techniques - IT network security - Part 2: Network security architecture	X	
ISO und IEC-NORMEN 18028-3:2005	Information technology - Security techniques - IT network security - Part 3: Securing communications between networks using security gateways	X	

Gesetz, VO, Norm, Regelung	Kurzbeschreibung	RM	SM,NM, KM
ISO und IEC-NORMEN 18028-4:2005	Information technology - Security techniques - IT network security - Part 4: Securing remote access	X	
ISO und IEC-NORMEN 18028-5:2006	Information technology - Security techniques - IT network security - Part 5: Securing communications across networks using virtual private networks	X	
ISO und IEC-NORMEN 18031:2005	Information technology - Securitytechniques - Random bit generatio	X	
ISO und IEC-NORMEN 18032:2005	Information technology - Security techniques - Prime number generation	X	
ISO und IEC-NORMEN 18033-1:2005	Information technology - Security techniques - Encryption algorithms- Part 1: General	X	
ISO und IEC-NORMEN 18033-2:2006	Information technology - Security techniques - Encryption algorithms - Part 2: Asymmetric ciphers	X	
ISO und IEC-NORMEN 18033-3:2005	Information technology - Security techniques - Encryption algorithms - Part 3: Block ciphers	X	
ISO und IEC-NORMEN 18033-4:2005	Information technology - Security techniques - Encryption algorithms - Part 4: Stream ciphers	X	
ISO und IEC-NORMEN 18043:2006	Information technology - Security techniques - Selection, deployment and operations of intrusion detection systems	X	x
ISO und IEC-NORMEN 18045:2008	Information technology - Security techniques - Methodology for IT security evaluation	X	x
ISO und IEC-NORMEN 19772:2009	Information technology - Security techniques - Authenticated encryption	X	x

Gesetz, VO, Norm, Regelung	Kurzbeschreibung	RM	SM,NM, KM
ISO und IEC-NORMEN 19785-4:2010	Information technology -- Common Biometric Exchange Formats Framework -- Part 4: Security block format specifications	X	x
ISO und IEC-NORMEN 19790:2006	Information technology - Security techniques - Security requirements for cryptographic modules	X	x
ISO und IEC-NORMEN 19792:2009	Information technology - Security techniques - Security evaluation of biometrics	X	x
ISO und IEC-NORMEN 21827:2008	Information technology - Systems Security Engineering - Capability Maturity Model (SSE-CMM)	X	x
ISO und IEC-NORMEN 2382-8:1998	Information technology - Vocabulary - Part 8: Security	X	x
ISO und IEC-NORMEN 24759:2008	Information technology - Security techniques - Test requirements for cryptographic modules	X	x
ISO und IEC-NORMEN 24761:2009	Information technology - Security techniques - Authentication context for biometrics	X	x
ISO und IEC-NORMEN 24762:2008	Information technology - Securitytechniques - Guidelines for informationand communications technology disasterrecovery services	Xx	x
ISO und IEC-NORMEN 24767-1:2008	Information technology - Home network security - Part 1: Security requirements	X	x
ISO und IEC-NORMEN 24767-2:2009	Information technology - Home network security - Part 2: Internal security services: Secure Communication Protocol for Middleware (SCPM)	X	x

Gesetz, VO, Norm, Regelung	Kurzbeschreibung	RM	SM,NM, KM
ISO und IEC-NORMEN 24824-3:2008	Information technology -- Generic applications of ASN.1: Fast infoset security	X	
ISO und IEC-NORMEN 27000:2009	Information technology - Security techniques - Information security management systems - Overview and vocabulary	X	
ISO und IEC-NORMEN 27001:2013	Information technology - Security techniques - Information security management systems - Requirements	X	
ISO und IEC-NORMEN 27002:2013	Information technology - Security techniques - Code of practice for information security management	X	
ISO und IEC-NORMEN 27004:2009	Information technology - Security techniques - Information security management - Measurement	X	
ISO und IEC-NORMEN 27005:2008	Information technology - Security techniques - Information security risk management	X	
ISO und IEC-NORMEN 27006:2007	Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management	X	
ISO und IEC-NORMEN 27011:2008	Information technology - Security techniques - Information security management guidelines for telecommunications organizations based on ISO/IEC 27002	X	
ISO und IEC-NORMEN 27019:2013	Leitfaden für das Informationssicherheits-Management von Steuerungssystemen der Ener-gieversorgung auf Grundlage der DIN ISO/IEC 27002	X	

Gesetz, VO, Norm, Regelung	Kurzbeschreibung	RM	SM,NM, KM
ISO und IEC-NORMEN 27031:2011	Information technology – Security techniques –Guidelines for information and communications technology readiness for business continuity	X	
ISO und IEC-NORMEN 27033-1:2009	Information technology - Security techniques - Network security - Part 1: Overview and concepts	X	
ISO und IEC-NORMEN 27035:2011	Information technology – Security techniques –Information security incident management	X	
ISO und IEC-NORMEN 27799:2008	Health informatics - Security management in health using ISO/IEC 27002	X	
ISO und IEC-NORMEN 7064:2003	Information technology - Security techniques - Check character systems	X	
ISO und IEC-NORMEN 7816-4:2005	Identification cards - Integrated circuit(s) cards with contacts - Part 4: Organization, security and commands for interchange	X	
ISO und IEC-NORMEN 9579:2000	Information technology - Remote database access for SQL with security enhancement	X	
ISO und IEC-NORMEN 9594-Parts 1-10:2008	Information technology - Open Systems Interconnection - The Directory	X	
ISO und IEC-NORMEN 9796-2:2002	Information technology - Securitytechniques - Digital signature schemegiving message recovery - Part 2: Integerfactorization based mechanisms	X	
ISO und IEC-NORMEN 9796-3:2006	Information technology - Security techniques - Digital signature scheme giving message recovery - Part 3: Discrete logarithm based mechanisms	X	

Gesetz, VO, Norm, Regelung	Kurzbeschreibung	RM	SM,NM, KM
ISO und IEC-NORMEN 9797-1:1999	Information technology - Security techniques - Message Authentication Codes (MACs) - Part 1: Mechanisms using a block cipher	X	
ISO und IEC-NORMEN 9797-2:2005	Information technology - Security techniques - Message Authentication Codes (MACs) - Part 2: Mechanisms using a dedicated hash-function	X	
ISO und IEC-NORMEN 9798-1:2010	Information technology - Security techniques - Entity authentication - Part 1: General	X	
ISO und IEC-NORMEN 9798-2:2008	Information technology - Security techniques - Entity authentication - Part 2: Mechanisms using symmetric encipherment algorithms	X	
ISO und IEC-NORMEN 9798-3:1998	Information technology - Security techniques - Entity authentication - Part 3: Mechanisms using digital signature techniques	X	
ISO und IEC-NORMEN 9798-4:1999	Information technology - Security techniques - Entity authentication - Part 4: Mechanisms using a cryptographic check function	X	
ISO und IEC-NORMEN 9798-5:2009	Information technology - Security techniques - Entity authentication - Part 5: Mechanisms using zero-knowledge techniques	X	
ISO und IEC-NORMEN 9798-6:2005	Information technology - Security techniques - Entity authentication - Part 6: Mechanisms using manual data transfer	X	
ISO und IEC-NORMEN TR 13594:1995	Information technology -- Lower layers security	X	

Gesetz, VO, Norm, Regelung	Kurzbeschreibung	RM	SM,NM, KM
ISO und IEC-NORMEN TR 14516:2002	Information technology - Security techniques - Guidelines for the use and management of Trusted Third Party services	X	
ISO und IEC-NORMEN TR 15067-4:2001	Information technology -- Home Electronic System (HES) Application Model -- Part 4: Security System for HES	X	
ISO und IEC-NORMEN TR 15443-1:2005	Information technology - Securitytechniques - A framework for IT securityassurance - Part 1: Overview andframework	X	
ISO und IEC-NORMEN TR 15443-2:2005	Information technology - Security techniques - A framework for IT security assurance- Part 2: Assurance methods	X	
ISO und IEC-NORMEN TR 15443-3:2007	Information technology - Security techniques - A framework for IT security assurance - Part 3: Analysis of assurance methods	X	
ISO und IEC-NORMEN TR 16166:2010	Information technology - Telecommunications and information exchange between systems - Next Generation Corporate Networks (NGCN) - Security of session-based communications	X	
ISO und IEC-NORMEN TR 18044:2004	Information technology - Security techniques - Information security incident management	X	
ISO und IEC-NORMEN TR 19791:2010	Information technology - Security techniques - Security assessment of operational systems	X	

Gesetz, VO, Norm, Regelung	Kurzbeschreibung	RM	SM,NM, KM
ISO und IEC-NORMEN TR 24714-1:2008	Information technology - Biometrics - Jurisdictional and societal considerations for commercial applications - Part 1: General guidance	X	
ISO und IEC-NORMEN TR 24729-4:2009	Information technology - Radio frequency identification for item management - Implementation guidelines - Part 4: Tag data security	X	
ISO und IEC-NORMEN TR 9564-4:2004	Banking - Personal Identification Number (PIN) management and security - Part 4: Guidelines for PIN handling in open networks	X	
ISO und IEC-NORMEN27003:2010	Information technology - Security techniques - Information security management system implementation guidance	X	
ISO und TR-NORMEN 11633-1:2009	Health informatics - Information security management for remote maintenance of medical devices and medical information systems - Part 1: Requirements and risk analysis	X	
ISO und TR-NORMEN 11633-2:2009	Health informatics - Information securitymanagement for remote maintenance ofmedical devices and medical informationsystems - Part 2: Implementation of aninformation security management system(ISMS)	X	
ISO/TS 17574:2009	Electronic fee collection - Guidelines for security protection profiles	X	

Gesetz, VO, Norm, Regelung	Kurzbeschreibung	RM	SM,NM, KM
ISO-NORMEN 9564-1:2002	Banking - Personal Identification Number (PIN) management and security - Part 1: Basic principles and requirements for online PIN handling in ATM and POS systems	X	
ISO-NORMEN 9564-2:2005	Banking - Personal Identification Number (PIN) management and security - Part 2: Approved algorithms for PIN encipherment	X	
ISO-NORMEN 9564-3:2003	Banking - Personal Identification Number (PIN) management and security - Part 3: Requirements for offline PIN handling in ATM and POS systems	X	
ISO und IEC 60870-5 Serie:2013	Telecontrol equipment and systems - Part 5: Transmission protocols, inkl. aller relevanter transmission protocols siehe IEC 60870-5-104 etc	X	
ISO und IEC 61850-1-10:Serie 2013	Communication networks and systems in substations Part 7-2: Basic information and communication structure – Abstract communication service interface (ACSI)	X	
ISO und IEC 61968 1-14: Serie 2013	Application integration at electric utilities - System interfaces for distribution	X	
ISO und IEC 61970-1-5:Serie 2013	Energy management system application program interface	X	

Gesetz, VO, Norm, Regelung	Kurzbeschreibung	RM	SM,NM, KM
ISO und IEC 62351:Serie 2013	Power systems management and associated information exchange - Data and communications security Part 1: Communication network and system security -Introduction to security issues Part 2: Glossary of terms Part 3: Communication network and system security – Profiles including TCP/IP Part 4: Profiles including MMS Part 5: Security for IEC 60870-5 and derivatives Part 6: Security for IEC 61850 Part 7: Network and system management (NSM) data object models	X	
ISO und IEC 62443-1-1:Serie 2013	Industrial communication networks – Network and system security – Part 1-1: Terminology, concepts and models	X	
ISO und IEC 62443-2-1:Serie 2013	Industrial communication networks- Network and system security – Part 2-1: Establishing an industrial automation and control system security program	X	
ISO und IEC 62443-2-4:Serie 2013 (früher ISA-99)	A Baseline Security Standard for Industrial Automation Control Systems	X	
IEC/PAS 62443-3	Security for industrial process measurement and control- Network and system security	X	
IEC/TR 62443-3-1	Industrial communication networks_ Network and system security – Part 3-1: Security technologies for industrial automation and control systems	X	
IEEE 1686-2007	Cyber Security Capabilities		

Gesetz, VO, Norm, Regelung	Kurzbeschreibung	RM	SM,NM, KM
ISA TRA99/IEC 62443	Security for Industrial Substation intelligent electronic devices /IED) Cyber Security Capabilities		
IEEE 1402	Guide for Electric Power Substation Physical and Electronic Security		
NERC Standard CIP-001-1	Sabotage Reporting	X	
NERC Standard CIP-002-1	Cyber Security -Critical Cyber Asset Identification	X	
NERC Standard CIP-003-1	Cyber Security-Security Management Controls	X	
NERC Standard CIP-004-1	Cyber Security-Personnel and Training	X	
NERC Standard CIP-005-1	Cyber Security-Electronic Security Perimeter(s)	X	
NERC Standard CIP-006-1	Cyber Security-Physical Security	X	
NERC Standard CIP-007-1	Cyber Security-Systems Security Management	X	
NERC Standard CIP-008-1	Cyber Security-Incident Reporting and Response Planing	X	
NERC Standard CIP-009-1	Cyber Security- Recovery Plans for Critical Cyber Assets	X	
NIST Special Publication 800-53	Recommended Security Controls for Federal Information Systems and Organizations	X	
NIST Special Publication 800-40 Version 2.0	Creating a Patch and Vulnerabilty Management Program	X	
NIST Special Publication 800-82	Guide to Industrial Control Systems (ICS) Security	X	

Gesetz, VO, Norm, Regelung	Kurzbeschreibung	RM	SM,NM, KM
NFPA 1600	Standard on Disaster/Emergency Management and Business Continuity Programs	X	
OHSAS 18001	Norm für Arbeits- und Gesundheitsschutz	Xx	
ÖNORM 2400 Business Continuity und Corporate Security Management	Business Continuity und Corporate Security Management	Xx	
ÖNORM 2410	Chancen- und Risikomanagement Analyse und Maßnahmen zur Sicherung der Ziele von Organisationen	Xx	
ÖNORM 2420	Industrieller Objektschutz	Xx	
ÖNORM B 3850	Brandschutztüren - Ein- und zweiflügelige Drehflügeltüren und -tore	X	
ÖNORM B 3855	Rauchabschlüsse - Einflügelige und zweiflügelige Drehflügeltüren aus Stahl oder Holz	X	
ÖNORM B 3858	Türschlösser - Einstemmschlösser (Einsteckschlösser) für Brandschutztüren	X	
ÖNORM B 5338	Einbruchhemmende Fenster, Türen und zusätzliche Abschlüsse - Allgemeine Festlegungen	X	
ÖNORM B 5453	Einbruchhemmende Türen - Hauptschlösser	X	
ÖNORM B 5455	Einbruchhemmende Türen - Schutzbeschläge für Hauptschlösser	X	
ÖNORM B 5456	Einbruchhemmende Türen - Zusatzschlösser	X	
ÖNORM B 5457	Einbruchhemmende Türen - Schließbleche für Hauptschlösser	X	
ÖNORM B 5458	Einbruchhemmende Türen - Bänder und Bandsicherungen	X	

Gesetz, VO, Norm, Regelung	Kurzbeschreibung	RM	SM,NM, KM
ÖNORM EN 1047-1	Wertbehältnisse - Klassifizierung und Methoden zur Prüfung des Widerstandes gegen Brand - Datensicherungsschränke	X	
ÖNORM EN 1047-2	Wertbehältnisse - Klassifizierung und Methoden zur Prüfung des Widerstandes gegen Brand - Datensicherungsräume und Datensicherungscontainer	X	
ÖNORM EN 1143	Wertbehältnisse - Anforderungen, Klassifizierung und Methoden zur Prüfung des Widerstandes gegen Einbruchdiebstahl	X	
ÖNORM EN 14450	Wertbehältnisse - Anforderungen, Klassifizierung und Methoden zur Prüfung des Widerstandes gegen Einbruchdiebstahl - Sicherheitsschränke	X	
ÖNORM ENV 1300	Wertbehältnisse - Klassifizierung von Hochsicherheitsschlössern nach ihrem Widerstandswert gegen unbefugtes Öffnen	X	
ÖNORM S 2109	Akten- und Datenvernichtung	X	
ÖNORMEN: A 7700	"Sicherheitstechnische Anforderungen an Webapplikationen" ist die erste zertifizierbare Norm im EU-Raum für die Sicherheit von Webanwendungen	X	
ONR 49000	Risikomanagement für Organisation und Systeme	xx	
RICHTLINIEN:			
Centre for the Protection of National Infrastructure	Process Control and SCADA Security Guide 1-7	X	

Gesetz, VO, Norm, Regelung	Kurzbeschreibung	RM	SM,NM, KM
Department of Homeland Security	Cyber Security Procurement Language for Control Systems	X	
EU 1999/93/EG	Richtlinie 1999/93/EG des europäischen Parlaments und des Rates vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen	X	
EU 5775/01]	Beschluss des Rates über die Annahme der Sicherheitsvorschriften des Rates	X	
Österreichischer Corporate Governance Code	Aufbau eines internen Kontrollsystems gilt für den Finanzsektor	X	
SKKM-Richtlinie BM für Inneres	Richtlinie für Krisen- und Katastrophenmanagement des Bundes	x	
Solvency II	Finanz. Riskmanagement	x	
DIN EN 61508	Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 1: General requirements (IEC 61508-1:2010); German version EN 61508-1:2010		
M/490	Standardization Mandate to European Standardisation Organisations (ESOs) to support European Smart Grid deployment		
ÖVE/ÖNORM EN 50518	Alarmempfangsstellen	X	
ÖVE/ÖNORM EN 50600-1:2013	Informationstechnik- Einrichtungen und Infrastrukturen von Rechenzentren	X	
ENISA	Recommended cryptographic measures – securing personal data		

Gesetz, VO, Norm, Regelung	Kurzbeschreibung	RM	SM,NM, KM
ENISA	Aktuelle „Activities zu“ http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/smart-grids-and-smart-meteringbdew		
BDEW Whitepaper	„Anforderungen an sichere Steuerungs- und Telekommunikationssysteme“ Deutschland 2009)		

Anhang 5: Abkürzungsverzeichnis

Abkürzung	Erklärung
AbwA	Abwehramt des BMLVS
AIT	Austrian Institute of Technology
AMI	Advanced Metering Infrastructure Headend
APCIP	Austrian Program Critical Infrastructure Protection
ASIDI	Average System Interruption Duration Index
B2B	Business 2 Business
CIRS	Critical Incident Reporting System
CIS	Customer Information System
COTS	Commericial off the Shelf
CSR	Customer Service Representative
DA	Distribution Automatisation
DCS	Distributed Control System
DER	Distributed Energy Resources
DMS	Distribution Management Systems
DRMS	Demand Response Management System
EMS	Energy Management System
EPCIP	European Program Critical Infrastructure Protection
ESP	Energy Service Provider
EUMD	Energy Usage Metering Device
EVUs	Energieversorungsunternehmen
GIS	Geographisches Informations System
HAN	Home Area Network
IDS	Intrusion Detection System
IED	Intelligent Electronic Device
IKT	Informations- und Kommunikationstechnologie
IPS	Intrusion Prevention System
ISO	Independent System Operator
KPI	Key Performance Indikator
KVP	kontinuierlicher Verbesserungsprozess
LMS	Load Management Systems
LMS/DRMS	Load Management Systems/Demand Response Management System
MDMS	Meter Data Management System
NB	Netzbetreiber
OMS	Outage Management System
ÖSCS	Österreichische Strategie zur Cybersicherheit
PEV	Electric Vehicle Service Element/Plug-in Electric Vehicle
PMU	Phasor Measurement Unit
RTO	Regional Transmission Organization Wholesale Market
RTO/ISO	Independent System Operator/Regional Transmission Organization Wholesale Market
RTU	Distribution Remote Terminal Unit
RZF	Regelzonenführer

Abkürzung	Erklärung
SAIDI	System Average Interruption Duration Index
SCADA	supervisory control and data acquisition
USV	Umfassende Sicherheitsvorsorge
WAMS	Wide Area Measurement System
WMS	Work Management System

Anhang 6: Übersicht der Quellen

Die gesamte Primärliteratur und Verweise sind auf der Begleit CD-R zusammengestellt und nach Schlagworten suchbar ! (vgl dazu auch Kapitel 4)

Übersicht der Literaturzusammenstellung:

Abbildung 12: Aufbau der Literaturzusammenstellung

Primärliteratur-Übersicht

Quellen, die im Internet oder sonst frei verfügbar sind, werden in der Literaturzusammenstellung als Dateien mit angeboten.

Abbildung 13: Dokumente in der Wissensbasis

Primärliteratur-Zitat

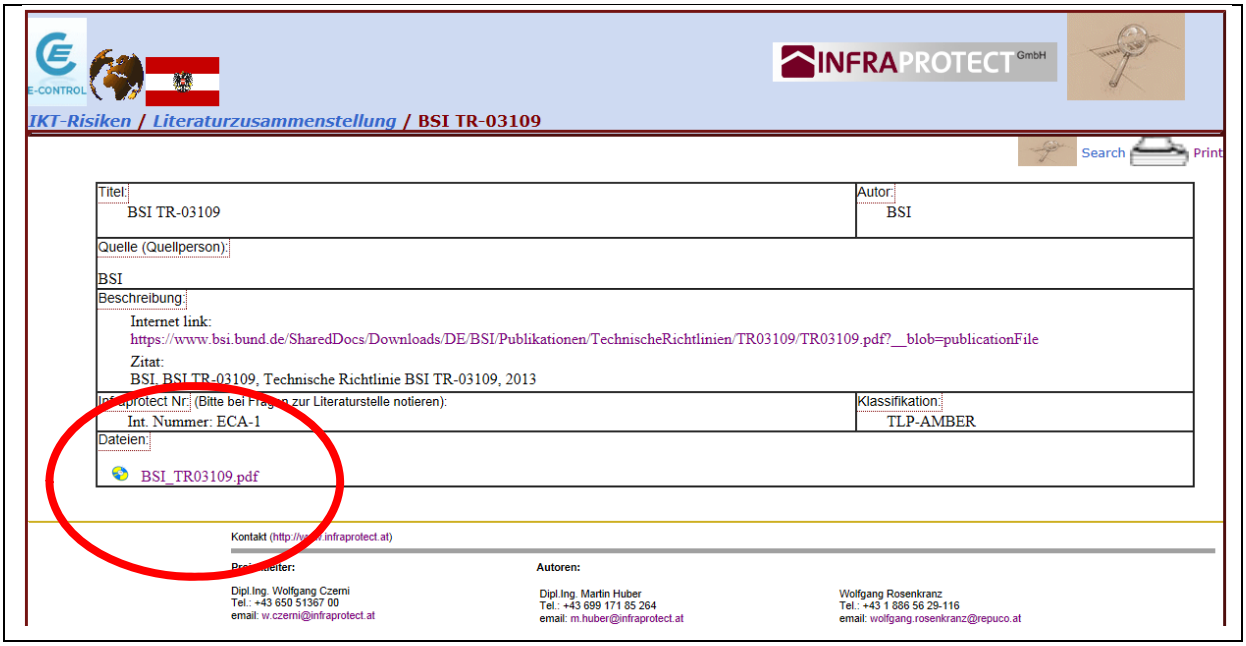


Abbildung 14: Dokumente in der Wissensbasis

Durch anklicken der Dateien werden die Originaldateien zur Verfügung gestellt.

Navigation

Um die Navigation in den Quellen zu erleichtern, wurde folgende Ordnungsstruktur eingeführt:

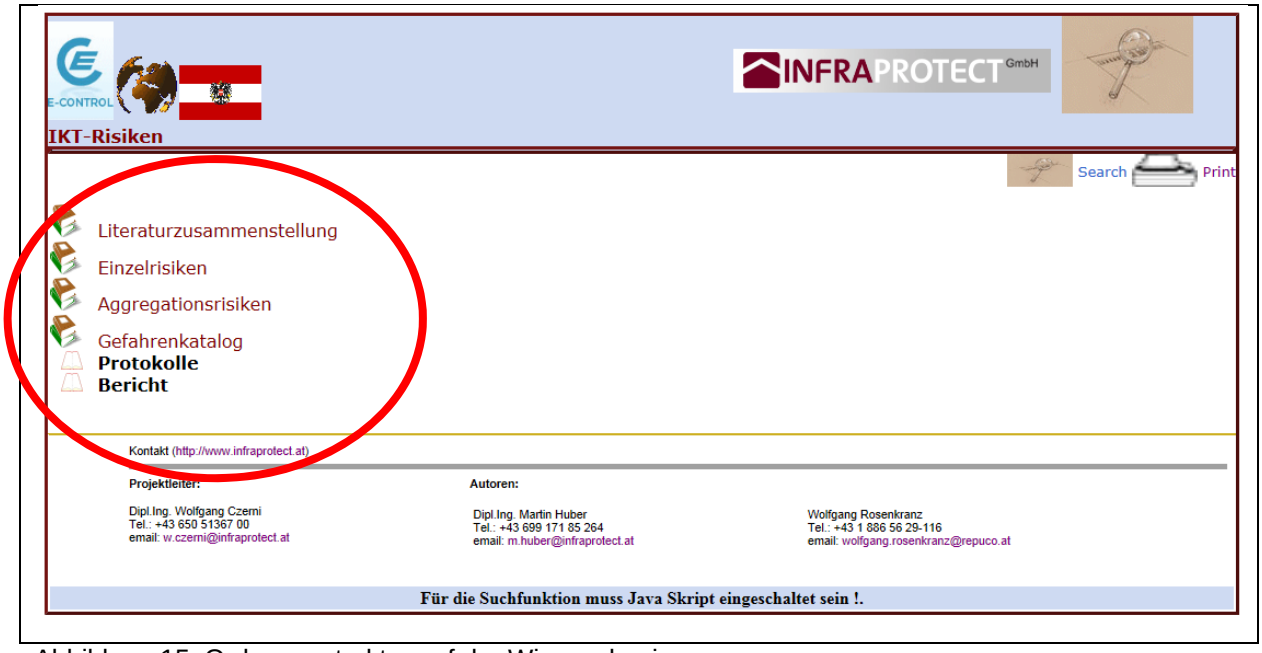


Abbildung 15: Ordnungsstruktur auf der Wissensbasis

Durch klicken auf „IKT-Risiken“ kommt man wieder auf die Übersicht retour.

Die Inhalte der CD-R können direkt in Ihr INTRANET/Internet übernommen werden!

Quellenangaben

Nachfolgende Quellen sind suchbar auf der CD-R zusammengestellt und wissenschaftlich zitiert.

1. Lit. ECA-13, Bundestagsdrucksache, die auf einen Bericht des Büros für Technikfolgen-Abschätzung beim Deutschen Bundestag basiert, Seite 32, Kapitel 2 Folgen für Kritische Infrastrukturen in Deutschland
2. Lit. ECA-16, Österreichische Ausfalls- und Störstatistik der E-Control
3. Lit. ECA-60, Apostel, Johannes Kepler Universität, übermittelt von Dr. Reichl, 16.04.13
4. Lit.ECA-61, ÖNORM S2401, Business Continuity und Corporate Security Management, “Systemaufbau und Business Continuity und Corporate Security Policy”
5. Lit. ECA-27, NIST Guidelines for Smart Grid Cyber Security: Vol1, Smart grid Cyber Security Strategy, Architecture and High-Level Requirements”
6. Lit. ECA-62, ebIX, Business Requirements and Information Models
7. Lit. ECA-06, BSI-Grundschutzkatalog
8. Lit. ECA-09, BSI-Sicherheit von Standleitungen
9. Lit. ECA-01, BSI: Technische Richtlinie BSI TR-03109-1 bis 5 (z.T. auch Drafts)
10. Lit.ECA-37, Öesterreichs Energie, Security im Smart Grid, Bericht(TLP-AMBER)
11. KPIs Key Performance Indikatoren
12. Lit.ECA-53, Appropriate security measures for smart grids, Guidelines to assess the sophistication of security measures implementation
13. Lit. ECA-32, Anforderungen an sichere Steuerungs- und Telekommunikationssysteme
14. Lit.ECA-62, ebIX, “Introduction to Business Requirements and Information Models”
15. Lit. ECA-44, Risikoanalyse Bereich ICT-Infrastruktur
16. Übertragungsnetz, Verteilnetz udg.
17. Lit. ECA-16, Ausfalls- und Störungsstatistik
18. Lit. ECA-34, Störung in leittechnischen Einrichtungen von österreichischen Übertragungs- und Verteilernetzbetreibern sowie bei Kraftwerksbetreibern 2. - 7. Mai 2013
19. Lit.ECA-54, ENISA, Recommendations-for-harmonized-ics-testing-capability-in-the-eu
20. Lit.ECA-36, VEÖ Empfehlung „Informationstechnik zur Bewältigung von Krisensituationen
21. Lit. ECA-06, BSI-Grundschutzkataloge
22. Lit. ECA-37, Security im Smart Grid
23. Lit.ECA-36, VEÖ Empfehlung „Informationstechnik zur Bewältigung von Krisensituationen

24. Lit.ECA-09, Sicherheitseigenschaften von Standleitungstechnologien, Kapitel 6.4.5.2 IP-Plattformlösung mit Verschlüsselung
25. Lit. ECA-55, Recommendation for Key Management – Part 1: General (Revision 3)
26. Lit. ECA-56, Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths"
27. Lit.ECA-36, VEÖ Empfehlung „Informationstechnik zur Bewältigung von Krisensituationen
28. Lit. ECA-37, Security im Smart Grid
29. Lit.ECA-58, NIST SP: 800-94, Guide to Intrusion Detection and Prevention Systems (IDPS)