INFRA PROTECT

»

Energie-Control Austria

Bericht

IKT-Risikoanalyse der Energiewirtschaft

Version 4.0-2021
ECA-OE-ÖVGW-WHITE-VERSION

Auftraggeber:
Energie-Control Austria

Aufgabensteller:
Dipl. Ing. Christian Schönbauer

Studienkennziffer:
entfällt

Gesamtzahl Seiten:
36

Anzahl Tabellen:
4

Anzahl Abbildungen:
12

Wien, 01.03.2021

Koordinierender Verfasser: DI Wolfgang Czerni, MBA

Management Summary

Im Jahr 2013 wurde ein Private-Public-Dialog (PPD) Prozess initiiert, der das Ziel verfolgt, eine in der Branche abgestimmte Sicht auf die Risikolandschaft bei der Nutzung von Informations- und Kommunikationstechnologien in der Energiewirtschaft zusammenzustellen, um daraus abgeleitete Risikominimierungsmaßnahmen abzustimmen. Dieser Prozess leistet einen entscheidenden Beitrag zur Umsetzung der Ziele des NIS-Gesetzes und soll bei der Implementierung von gemeinsam definierten Sicherheitsstandards unterstützen. Dazu wurde ein Arbeitsgremium, bestehend aus Vertretern der Ministerien BKA, BM.I, BMLV, BMK, der E-Control (ECA), dem Austrian Energy CERT (AEC), den Interessensvertretungen der Elektrizitäts- und Gaswirtschaft sowie aus Experten aus den wesentlichen Netzbetreibern, Kraftwerksbetreibern sowie Speicherbetreibern zusammengestellt. In der aktuellen Fassung der Risikobetrachtungen wurde erstmals auch ein Schritt hin zu Einbindung von Betreibern Wesentlicher Dienste aus der Telekommunikationsbranche vollzogen. Hier wurden in einem Initialprozess mögliche Abhängigkeiten und Kaskadeneffekte von und mit der Telekommunikationsbranche identifiziert. Dieser Prozess wurde durch die beiden Regulierungsbehörden E-Control und der Rundfunk und Telekommunikations Regulierungsbehörde RTR koordiniert. Der Bericht fasst die Ergebnisse aller betrachteten Risiken der Elektrizitäts- und Gaswirtschaft sowie erster Kaskadeneffekte mit der Telekombranche zusammen. Dazu wurde das Risikoportfolio in mehrere Teilaspekte aufgetrennt, um eine detaillierte Sicht auf verschiedene Einzelrisiken zu gewährleisten. Es sind dies die Risikokategorien:

- Design- und Architektur der IKT
- Eskalation und Kommunikation
- Hard- und Software
- Faktor Mensch
- Naturgefahren
- Normung und Recht
- Organisatorische Sicherheit
- Planungs- und Beschaffungsprozesse
- Zugriffskontrolle und Kryptographie

Zur Risikoreduktion wurden Empfehlungen aus zwei wesentlichen Blickwinkeln heraus abgeleitet:

Empfehlungen, die sich an die Unternehmensprozesse richten:

- Sicherstellung eines resilienten inter- und intraorganisatorischen Business Continuity- und Krisenmanagements, u. a. auch durch regelmäßige Teilnahme an Übungen unter Einbindung des AEC.
- Die Implementierung eines holistisch ausgeprägten Sicherheits-Managementsystems, welches auf dem Fundament der ISO 27.001, ergänzt um die Branchennorm ISO 27.019 sowie den Empfehlungen des BDEW-OE-White-Papers aufgebaut wird. Wobei neben den durch die NISG bzw. NISV definierten „Scopes“ die gesamte Sicherheitskette entlang aller Phasen der Produkt-Life-Cycles von IKT-Equipment betrachtet werden soll.

Empfehlungen zur Weiterentwicklung des „Stands der Technik“:

- Einbindung des Sachverstands Österreichischer Unternehmen, Interessensvertretungen und Behörden in den EU-weiten Prozess der Fortentwicklung von Standards, Richtlinien und Testregimen, um den kommenden raschen Weiterentwicklungen in der IKT einen entsprechend ausgeprägten Technologiefolgeabschätzungsprozess entgegenstellen zu können. Damit verbunden sind Empfehlungen zur Sicherstellung der Versorgungssicherheit bei der Integration erneuerbarer Energieinfrastrukturen.

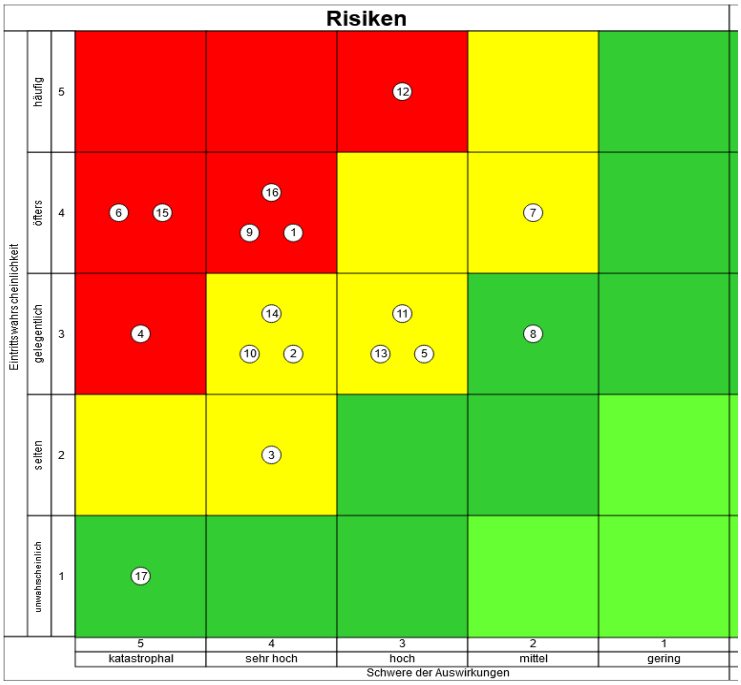
Kurzfassung

Der vorliegende Bericht fasst die Ergebnisse des Updateprozesses der IKT-Risikoanalyse Version 3.0 im Zeitraum Jänner bis Dezember 2020 zur vorliegenden Version 4.0 zusammen. Im Wesentlichen werden vier Schwerpunkte beschrieben.
Im Teil I wird die Methodik und Vorgehensweise der Aktualisierung auf Basis der bereits bekannten Methodik kurz wiederholend beschrieben.
Der Teil II beschäftigt sich mit der Aktualisierung der Kommunikationsgeflechte in Strom und Gas. Diese wurden komplett neu überarbeitet. Auf die Beschreibung des Gefahrenkatalogs wird verzichtet, da dieser umfassend bereits in der Version 3.0 zusammengestellt wurde. Die darin beschriebenen Gefahren wurden an die neuen und geänderten Bedingungen angepasst. Es sind keine zusätzlichen Gefahren mit in den Katalog aufgenommen worden.
Teil III widmet sich der Zusammenfassung der wesentlichen Ergebnisse des Risikoidentifikations- und Bewertungsprozesses. Die harmonisierten Risiko-Bewertungskriterien, die Einzel- und Aggregationsrisiken sowie die dennoch verbleibenden stromspezifischen Einzelrisiken werden sowohl einzeln als auch in den Anhängen detailliert aufbereitet. Die Aggregationsrisiken werden eingehender diskutiert. (In den erarbeiteten Maßnahmen wurde TK berücksichtigt bzw. integriert.) In diesem Teil wird auch der begonnene Abstimmungsprozess mit der Telekommunikationsbranche im Rahmen der Diskussion um Kaskadeneffekte beschrieben. Hier werden auch die aus Sicht der Telekommunikation und Energiewirtschaft relevanten gemeinsamen Risiken und Kaskadeneffekte diskutiert.
Teil IV beschäftigt sich mit den abgeleiteten übergeordneten Empfehlungen der Weiterentwicklung von Cybersicherheit für die Energiewirtschaft aus inter- und intraorganisatorischer Sicht.

In Summe wurden in sechs, jeweils ca. 6 Stunden dauernden Arbeitsworkshops 71 gemeinsame, für Strom und Gas relevante Risiken identifiziert. Auch die 19 stromspezifischen Einzelrisiken wurden im Rahmen des Updateprozesses evaluiert. Die 71 gemeinsamen Einzelrisiken wurden in mehreren Iterationen zu 17 Aggregationsrisiken zusammengefasst. Grundsätzlich wurden zwei Risikosichten gewählt: einmal die primär betriebliche Sicht mit Blick auf die Versorgungssicherheit in der Energiewirtschaft und einmal eine reputative Sicht auf Störungen aller Art. Alle Risiken wurden in einem „Worst Case“, „Best Case“ und selbstverständlich in einer Erwartungssicht, dem „Most Likely“ bewertet.

Den Einzelrisiken (inkl. der stromspezifischen) wurden 9 Risikokategorien zugeordnet, die auch das primäre, aber nicht ausschließliche Aggregationskriterium darstellen. Innerhalb dieser Risikokategorien wurden 27 Empfehlungen erarbeitet, die mehreren Stakeholdern zugeordnet wurden. Um die Maßnahmenumsetzung und Verfolgung zu erleichtern, hat die Expertengruppe für alle Empfehlungen einen Prozesseigner vorgeschlagen, der in ebenfalls bereits drei vordefinierten Zukunftshorizonten die Umsetzungen der Empfehlungen koordinieren bzw. katalysieren sollte.

Für die Darstellung der 17 Aggregationsrisiken wurde der „Worst Case“ herangezogen. Aus dieser Perspektive heraus wurden 7 hohe Risiken, 8 mittlere Risiken und zwei geringe Risiken identifiziert. Nachfolgend werden primär die hohen Risiken näher beschrieben.



Risikonummern im roten Bereich stellen „hohe Risiken“ dar.

Risikonummern im gelben Bereich stellen „mittlere Risiken“ dar.

Risikonummern im grünen Bereich stellen im Vergleich „geringe Risiken“ dar.

Abbildung 1: Worst Case Risiken

Die hohen Risiken tragen dem Umstand Rechnung, dass Cyberattacken gegen kritische Infrastrukturen[1] zunehmend mit höherer Expertise bzw. „Qualität“ ausgeführt werden. Hier werden hohe Schadenspotentiale durch bis dato unerkannte Schwachstellen bei Core-Komponenten unterstellt. Risiken im mittleren Bereich beschäftigen sich im Wesentlichen mit dem Faktor Mensch, die die Wiederherstellungszeiten eines „Regelbetriebes“ bei Schadereignissen stark beeinflussen. Technische Ausfälle von kritischen Komponenten in der Sensor-Steuerungs- und Aktorenkette sowie die Abhängigkeiten von qualitativ hochwertiger Beschaffung von Komponenten, die für den Betrieb signifikante funktionale Sicherheitsmerkmale aufweisen, werden als „mittleres Risiko“ betrachtet. Parallel dazu kann man Risiken, die durch eingeschränkte Auswertungen und Informationsverteilungen von "Beinahestörungen" von/bei IKT-Störereignissen entstehen in den „grünen Bereich“ verschieben. Dies wurde durch die Einrichtung und Begleitung eines Austrian Energy CERTs (AEC) möglich. Gefahren, die vom Einsatz kryptographischer Verfahren und Prozesse ausgehen können, werden als geringes Risiko eingestuft.

Die Aggregationsrisiken wurden im Vergleich zur Version 3.0 aus 2018 um ein Risiko ergänzt bzw. es entstand durch Umstrukturierungen bei der Aggregation. Die Risikoverteilung zwischen hohen, mittleren und geringen Risken hat sich jedoch kaum verändert. Zwei Risiken konnten durch die bereits umgesetzten Maßnahmen geringer bewertet werden. Hier wird die Effektivität des Prozesses herausgestrichen, die zu jedem Einzel- und Aggregationsrisiko Minimierungsmaßnahmen vorsieht. Risiken werden als denkbare Möglichkeiten definiert. Viele Risikominimierungsmaßnahmen sind in den meisten Unternehmen bereits umgesetzt.

Die Ergebnisse wurden in einer großen Expertengruppe, bestehend aus Vertretern verschiedener Organisationsgrößen von Netz- und Kraftwerks-, sowie Speicherbetreibern, Interessensvertretungen von Strom und Gas sowie unter aktiver Beteiligung von BMLV und BM.I, dem Austrian Energy CERT (AEC) sowie der E-Control erarbeitet. Die E-Control fungiert dabei als Prozesseigner des gesamten Private-Public-Dialog-Prozesses. Im Jahr 2020 wurde die Mehrheit der Workshops im Rahmen von Videokonferenzen durchgeführt.

[1] Siehe ECA-25, Bericht Cybersicherheit 2020, Kap. 1.1

Inhalt

Abbildungsverzeichnis

Tabellenverzeichnis

Teil I Methodik und Kontext

1. Grundsätzlicher Aufbau der Risikoanalyse

Die vorliegende Risikoanalyse ist methodisch analog zur V3.0-2018 aufgebaut. Sie 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 risk management", „ISO 31.010 risk assessment techniques" und der ONR 49.002-2, „Risikomanagement für Organisationen und Systeme, Leitfaden für die Methoden der Risikobeurteilung".
- Der Teil II stellt die Ergebnisse der Überarbeitung der beiden Domänenmodelle zusammen.
- Im Teil III, Ergebnisdarstellung, werden die Anpassungen und Erweiterungen der Aggregationsrisiken und der Einzelrisiken aufbereitet. Zusätzlich werden die identifizierten gemeinsamen Risken mit der Telekommunikationsbranche und daraus abgeleitet mögliche Kaskadeneffekte diskutiert.
- Aus der Zusammenschau aller Einzel- und Aggregationsrisiken wurden Maßnahmen & Empfehlungen abgeleitet, die im Teil IV aufbereitet sind.

Alle Details werden in den entsprechenden Anhängen aufbereitet. Die dazu erarbeiteten Datengrundlagen werden auf dem Expertenportal der E-Control https://share.e-control.at strukturiert abgelegt. An dieser Stelle sei nochmals der Hinweis gegeben, dass die vorliegenden Risikobetrachtungen als TLP-AMBER klassifiziert wurden.

2. Zielsetzungen der Aktualisierung der Risikoanalyse

2.1 Allgemeines

Die allgemeinen Ziele und Nichtziele des Risikoanalyseprozesses wurden nicht verändert. Hauptziel der Arbeitsgruppe ist es, sich verändernde Gefahren, die durch die Nutzung und Anwendung von Informations- und Kommunikationstechnologie in der Energiewirtschaft determiniert sind, zu erkennen und zu entsprechenden Risiken zu bewerten. In der Auswirkung solcher „Gefahren" stehen ein **nennenswerter** und **flächendeckender** Stromausfall bzw. entsprechend **signifikante Liefereinschränkungen** im Gas im Fokus. Gefahren können dabei grundsätzlich durch:

- technische Implementierungen,
- menschliche Fehlleistungen,
- Natur- und Elementarereignisse sowie durch
- kriminelle und/oder terroristische Aktivitäten (Intentionale Gefahren) bedingt sein.

Im Sinne der Nutzung der IKT stehen daher:

- Verfügbarkeit
- Integrität und
- Vertraulichkeit

im Mittelpunkt der Bewertungen.
Finanzielle bzw. betriebswirtschaftliche Gefahren für Betreiber der IKT-Systeme bei Strom- und Gasnetzen, Erzeugungsanlagen, Gasspeichern sowie auch von Handelsplattformen werden nur dann berücksichtigt, wenn in der mittelbaren Schadwirkung die Gefahr eines **nennenswerten** und **flächendeckenden** Stromausfalls bzw. **nennenswerte Liefereinschränkungen** in der Gasversorgung bestehen.

2.2 Zielsetzungen der Aktualisierung

Die Ziele der aktuell vorliegenden Evaluierung der IKT-Branchenrisikoanalyse können wie folgt zusammengefasst werden:

- Grundsätzliche Evaluierung der bestehenden Einzel- und Aggregationsrisiken. Eine Überprüfung der Risikobewertung wird hier als zwingend erachtet, da Maßnahmen zur Risikominimierung im Rahmen des kontinuierlichen Verbesserungsprozesses bei den Organisationen implementiert werden bzw. bereits wurden.
- Andere Branchen haben inzwischen einen ähnlichen Gefahrenidentifikations- und Bewertungsprozess durchlaufen. Insbesondere die auf der Hand liegenden Interdependenzen zwischen der Telekommunikationsbranche und der Energieversorgungsindustrie erzwingen einen intensiveren Informationsaustausch. Dieser wurde im Rahmen dieses Evaluierungsschrittes erstmals begonnen und wird fortzusetzen sein.

Das Verfahren der Gefahrenidentifikation und -bewertung wird als Risikomanagementprozess im Rahmen eines Privat-Public-Dialogs (PPD) verstanden. Eine wiederkehrende Evaluierung der Ergebnisse ist daher notwendig. Die Periodizität richtet sich hier nach aktuellen Entwicklungen, wird durch den Lenkungsausschuss determiniert und im Rahmen von Expertenworkshops umgesetzt. Mit Blick auf einen kontinuierlichen Verbesserungsprozess wurde eine Anlehnung der Aktualisierungsperiode an das Audit-Regime der ISO 27.001 ins Auge gefasst.
Für die vorliegenden Betrachtungen, insbesondere für die Zusammenstellung der Empfehlungen wurde ein Prognosehorizont bis 2025 vereinbart.

Ein weiteres Ziel der Evaluierung der bereits erarbeiteten Empfehlungen ist es, erste Aufwandsschätzungen für die Implementierung und Fortschreibung der hier zusammengefassten Maßnahmen & Empfehlungen aufzuzeigen, um damit auch Transparenz für die zum Teil erheblichen Security-Kosten zu schaffen.

2.3 Kontext der Risikoanalyse

Die gesamte Genese der vorliegenden Risikobetrachtungen ist durch einen konsensualen Private-Public-Dialog gekennzeichnet. Die sich aus den Einzel- und Aggregationsrisiken ergebenden Maßnahmen zur Risikominimierung wurden auf Basis eines rein technisch-organisatorischen Diskurses erarbeitet.

2.3.1 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 Lagever-

ständnis 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.

2.3.2 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 zum Schutz strategisch wichtiger Unternehmen in Österreich (APCIP).
Als eine Umsetzung der Vorgaben des APCIP wird die Entwicklung der IKT-Sicherheitsstrategie angesehen.

2.4 Umsetzung der NISG und NISV

Mit dem 2013 veröffentlichten Vorschlag für eine „Richtlinie des Europäischen Parlaments und des Rates vom 06.07.2016 über Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit in der Union", kurz NIS-Richtlinie muss Österreich die Vorgaben dieser Richtlinie bis zum 09. Mai 2018 umsetzen. Die Umsetzung erfolgte mittels des Bundesgesetzes zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystemsicherheitsgesetz – NISG, BGBl I Nr. 111/2018) und der unmittelbar zugeordneten Verordnung NISV (BGBl II Nr. 215/2019). Im Wesentlichen betrifft die Energiewirtschaft der §4 der NISV, Wesentliche Dienste, Sektor Energie. Mit dem Inkrafttreten des NISG bzw. der NISV, werden hier auch Mindestsicherheitsstandards definiert und in weiterer Folge durch „Qualifizierte Stellen" auditiert.
Ziel dieses hier vorliegenden PPD-Prozesses ist es, die Mindestsicherheitsstandards, die in den Mappingtabellen der NISV in Form von Fact-Sheets veröffentlicht werden, für die Energiewirtschaft durch einen gemeinsamen Erarbeitungsprozess mit der NIS-Behörde auszugestalten.
In diesem Zusammenhang sollen auch die o. a. NIS-Auditkriterien der Sicherheitsstandards mitgestaltet werden. In diesem Kontext spielt der hier beschrittene PPD-Prozess eine wesentliche Rolle, da durch konkrete Festlegung von Maßnahmen de facto ein Branchensicherheitsstandard mitdefiniert werden kann. Um diesem Anspruch gerecht zu werden, wurden wesentliche Normen und Regelungen zusammengestellt.

3. Methodik der Risikoanalyse

Der PPD-Prozess entspricht normativen Vorgaben zum Risikomanagement[2]. Um dem PPD-Gedanken entsprechend Rechnung zu tragen, wurden seitens der E-Control (ECA) zwei maßgebliche Projekt- und Arbeitsgruppen eingerichtet:

- Ein Lenkungsausschuss (LSA), der die Schnittstelle zur Österreichischen Cyber Security Strategie (ÖSCS), zur Österreichischen Sicherheitsstrategie (USV), zur Cybersecurity Plattform (CSP) und zum Österreichischen Programm zum Schutz kritischer Infrastrukturen (APCIP) darstellt.

Das Expertengremium besteht aus Vertretern von Netz-, Kraftwerks- und Speicherbetreibern. Für eine allgemeine Risikobetrachtung, die alle Aspekte der Ziele der Branchenrisikoanalyse abdecken soll, wurde eine geeignete Abstufung der Signifikanz von Auswirkungen auf die Netz-, Kraftwerks-, und Speicherbetreiber im Rahmen der Workshops erarbeitet. Die Ergebnisse der Betrachtungen sollen für alle Organisationsgrößen vergleichbar bleiben bzw. sein. Im Rahmen der Risikobewertungen müssen Aussagen zu „Erwartungswerten" für Stör- oder Schadereignisse prognostiziert oder besser abgeschätzt werden. Wie bereits erwähnt, wurde der Prognosehorizont für die Erfassung und Bewertung von Risiken mit 2025 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. Hier wurde der Begriff der Machbarkeit eingeführt und durch die Risikobewertungskriterien so abgestuft, dass daraus eine einheitliche Risikomatrix zusammengestellt werden kann. Eine Herleitung der Risikobewertungskriterien wird im Kapitel Allgemeines zur Herleitung der Bewertungskriterien zusammengefasst.
Es ist in diesem Zusammenhang wichtig darauf hinzuweisen, dass die identifizierten und bewerteten Risiken immer nur **in Relation zueinander** eine valide Aussage erlauben. Es wird nicht der Anspruch erhoben, dass die identifizierten Risiken eine *absolute* Position in der Risikomatrix einnehmen.

[2] Siehe ONR 49.002-1-2, ISO. 31.000 und ISO 31.010

3.1 Allgemeine Übersicht des Risikoidentifikationsprozesses

Der Risikoerfassungs- und Risikobewertungsprozess wurde gemäß Abbildung 2 durchgeführt.

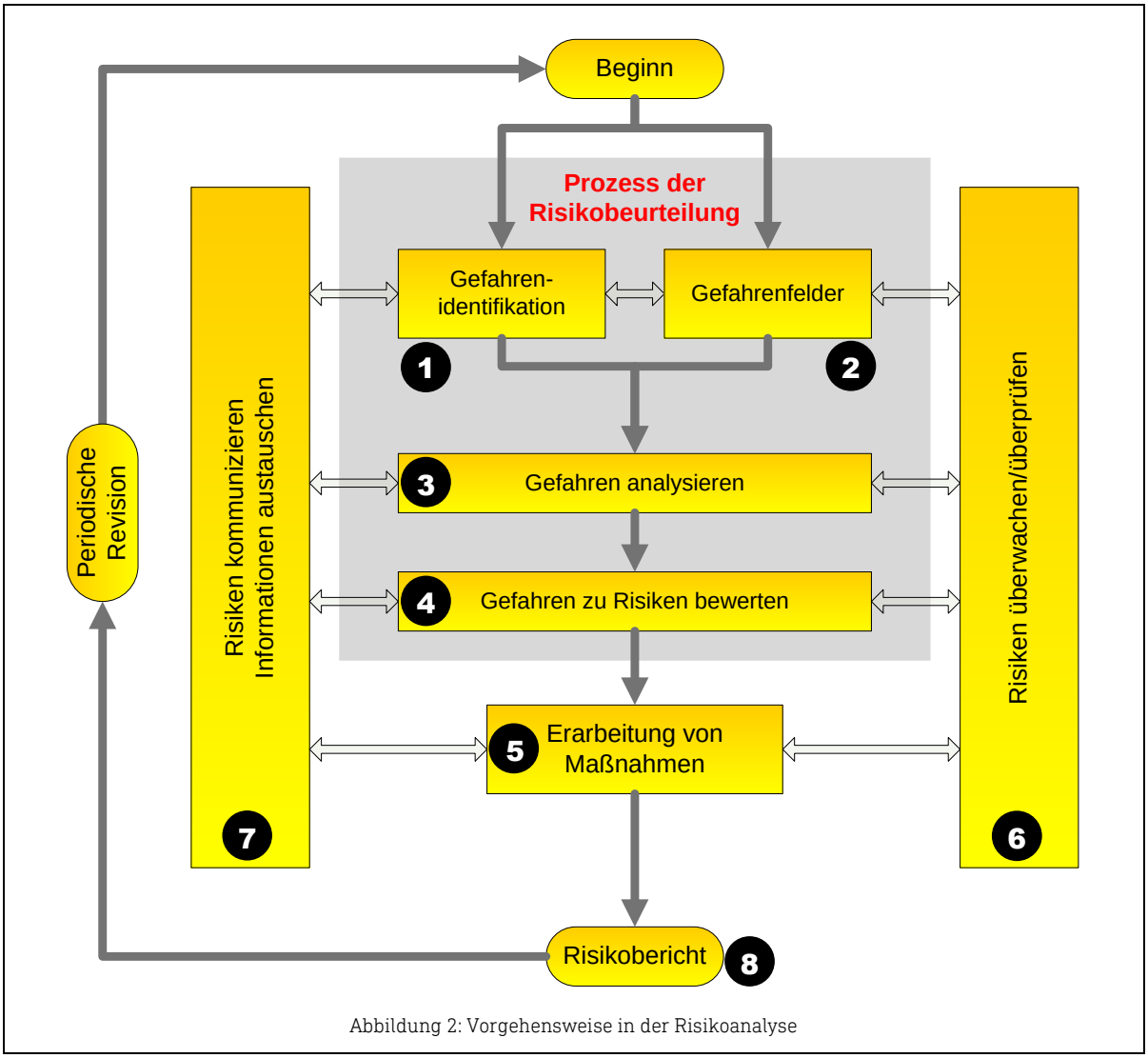


Abbildung 2: Vorgehensweise in der Risikoanalyse

3.1.1 PROZESSSCHRITT 1 GEFAHRENIDENTIFIKATION

Der Gefahrenidentifikationsprozess geht davon aus, dass Kommunikation in:

- Verfügbarkeit
- Vertraulichkeit und
- Integrität

gestört werden kann bzw. wird. Als wesentlichster Schritt wird die Erarbeitung eines umfassenden Kommunikationsgeflechts erachtet, wobei parallel dazu bestehende Gefahrenkataloge als Grundlage für die Gefahrenidentifikation herangezogen wurden.

3.1.2 PROZESSSCHRITT 2, GEFAHRENFELDER

Die im Prozessschritt 1 erarbeiteten Gefahren wurden im Strom-Domänenmodell in 16 verschiedenen Gefahrenfeldern=Domänen und im Gas-Domänenmodell in 12 verschiedenen Kommunikationsgeflechten zusammengestellt. Diese Analyse stellt die Grundlage für die systematische Identifikation von Risiken. Als Basis für die Überarbeitungen der Domänenmodelle wurden die in der Version 3.0-2018 erarbeiteten Kommunikationsbeziehungen herangezogen und an die neuesten Erkenntnisse angepasst. Basierend auf den verschiedenen Kommunikationsgeflechten wurden die entsprechenden Gefahren diskutiert und anhand der bestehenden Risikolandschaft Risiken neu bewertet.

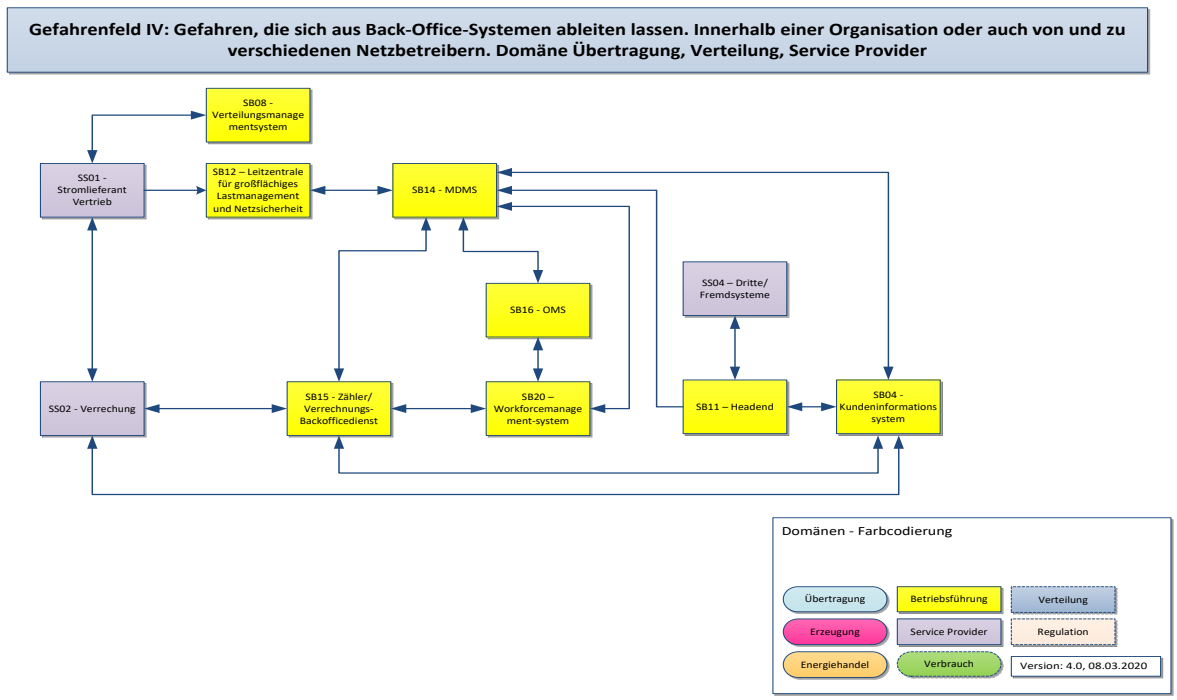


Abbildung 3: Kennzeichnung neu hinzugekommener Kommunikationsstrukturen

Anhand solcher Kommunikationsgeflechte wurden mögliche Risiken identifiziert und bewertet.

3.1.3 PROZESSSCHRITT 3, GEFAHRENANALYSE

In den jeweiligen Domänen wurden während der Workshops auf Basis der gesammelten Erfahrungen der letzten beiden Jahre zusätzliche Gefahren in die Gefahrenfelder eingearbeitet und analysiert. Im Rahmen des Überarbeitungsschrittes wurde auch versucht, die Interdependenzen zu verdeutlichen. Es wurde jedoch sehr schnell deutlich, dass die Domänenmodelle aufgrund der in sich geschlossenen Netztopologien wenig direkte Kommunikationsbeziehungen aufweisen. Schnittstellen wurden primär in den gesamten Bilanzierungsprozessen sowie bei „Überwachungs- und Monitoringprozessen“ gefunden, die bei Störungen mögliche Schadwirkungen kaskadieren könnten. Schwerpunkt der Risikobetrachtungen sind jedoch primär Szenarien, die durch technische oder durch intentional ausgenutzte Schwachstellen in Komponenten oder „vernetzten Systemen“ Auswirkungen auf die Steuerungssysteme haben. Die Auswirkungen auf Speicher-, Erzeugung und Netzbetrieb wurden daher primär auf der technisch-organisatorischen Ebene betrachtet und weniger unter den Gesichtspunkten der Betriebsführung selbst.

3.1.4 PROZESSSCHRITT 4, BEWERTUNG VON RISIKEN

Das Risiko wird als Produkt von Eintrittswahrscheinlichkeit mal 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 Grundlage der Risikobewertungen)
- Phase II, Bewertung der identifizierten Gefahren zu 71 Einzelrisiken, wobei die Risiken in mehrfacher Hinsicht bewertet wurden. Einerseits einmal in der reinen Bewertung der drei Dimension Verfügbarkeit, Vertraulichkeit und Integrität und einmal mit Blick auf die Verteilung der Bewertung durch Betrachtung von Extremfällen „Best Case" und „Worst Case" sowie mit Blick auf einen „Erwartungswert", dem „Most-Likely"
- Phase III, Aggregation der 71 Einzelrisiken zu 17 Aggregationsrisiken

In einer gesonderten Phase wurden die residualen stromspezifischen Risiken neu bewertet.

3.1.5 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.

3.1.6 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.

3.1.7 PROZESSSCHRITT 7, RISIKOBERICHT

Der vorliegende Risikobericht fasst den abgestimmten Sachstand mit 12.12.2020 zusammen.

3.1.8 PROZESSSCHRITT 8, PERIODISCHE REVISION

Die Risikoänderungen sind durch Umsetzung von Maßnahmen entsprechend zu erfassen, um den kontinuierlichen Verbesserungsprozess (KVP) zu dokumentieren. An dieser Stelle sei darauf hingewiesen, dass eine Risikoanalyse lediglich eine Teilaufgabe eines kontinuierlichen Verbesserungsprozesses darstellt.
Wie bereits erwähnt soll sich der Revisionszyklus der vorliegenden Risikoanalyse an dem Auditregime der ISO 27.001 orientieren.

Teil II Kommunikationsgeflechte

4. Domänenmodell.at

4.1 Domänenmodell.at-Strom

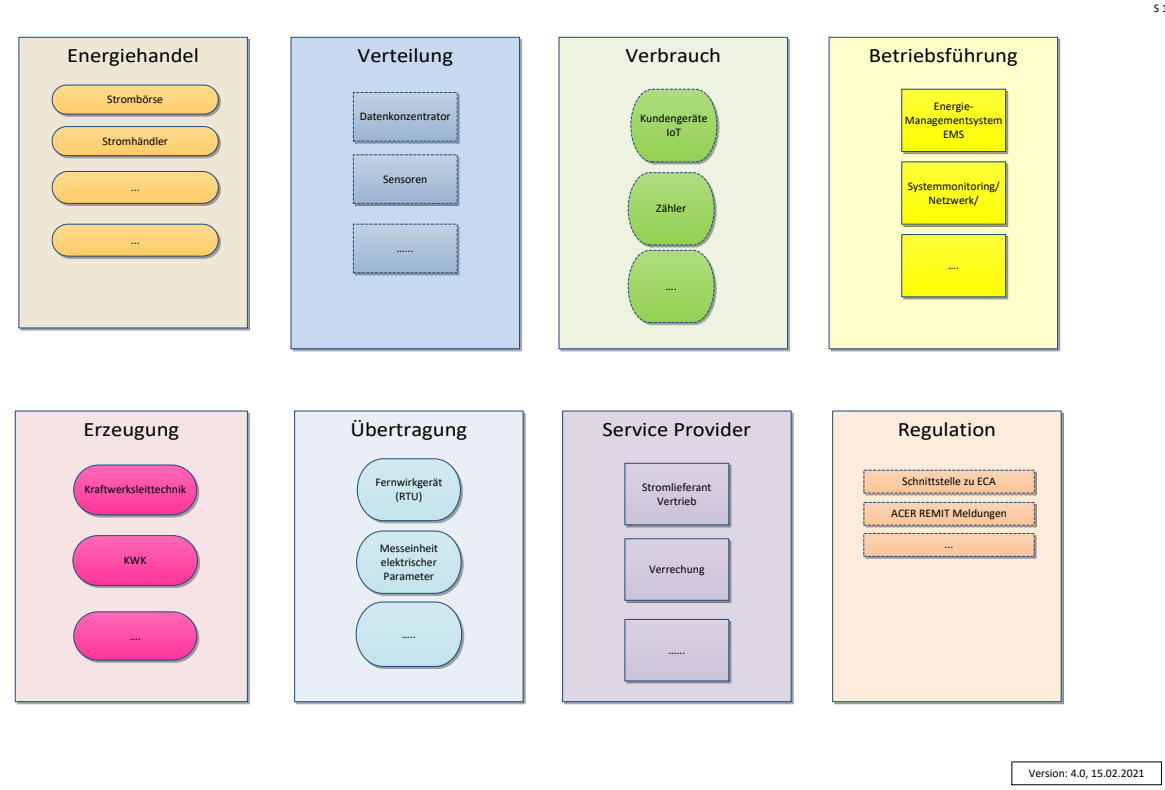


Abbildung 4: Arbeitsgruppierung kommunikativ-funktionaler Zusammenhänge

In Anlehnung bzw. abgeleitet aus dem NIST-Domänenmodell wurden in der Version 1.0 der IKT-Risikoanalyse Strom folgende Gruppen funktionaler Einheiten zusammengefasst:

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

Durch die Komplexität der technisch-organisatorischen Kommunikationsbeziehungen ist eine eindeutige 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. Die „Vereinfachung" der Komplexität wird durch Aufteilung ALLER Kommunikationsbeziehungen in 16 verschiedene Sichten versucht. Diese Analyse dient dazu, mögliche Gefahren anhand der Kommunikationsbeziehungen besser identifizieren zu können. Das gesamte Kommunikationsgeflecht wird daher in 16 Gefahrenfelder=Domänen eingeteilt. Es sind dies:

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

» Gefahrenfeld Strom XVI: Gefahren, die sich aus der Nutzung von „Elektronischen Datenaustauschplattformen“ ableiten lassen.

4.2 Domänenmodell.at-GAS

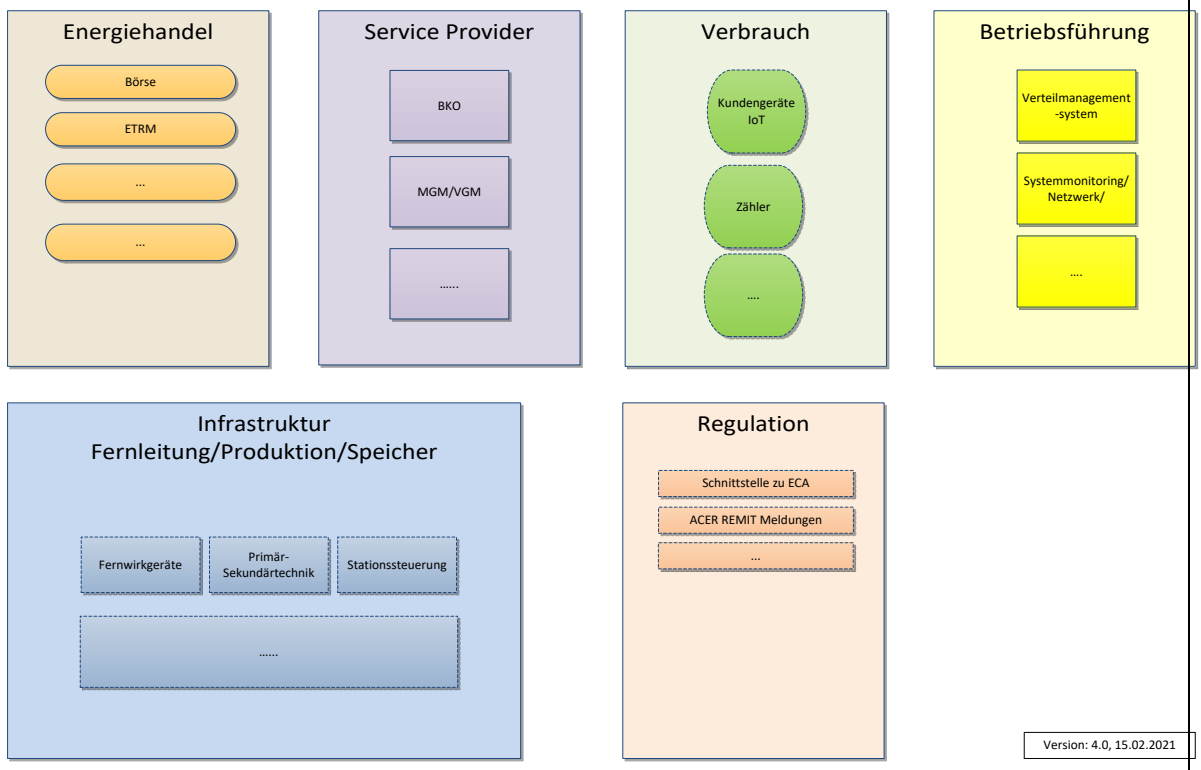


Abbildung 5: Arbeitsgruppierung kommunikativ-funktionaler Zusammenhänge

Das Domänenmodell fasst folgende Gruppen funktionaler Einheiten zusammen:

» Infrastruktureinrichtungen

» Entitäten in der Betriebsführung

» Entitäten des Energiehandels

» Entitäten aus Sicht von Service Providern

» Entitäten im Verbrauch

» Aspekte im regulierten Markt

Analog zu dem Domänenmodell .at-Strom ist eine eindeutige 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. Die „Vereinfachung“ der Komplexität wird durch Aufteilung ALLER Kommunikationsbeziehungen in 16 verschiedene Sichten versucht. Diese Analyse dient dazu, mögliche Gefahren anhand der Kommunikationsbeziehungen besser identifizieren zu können. Das gesamte Kommunikationsgeflecht wird daher in 12 Gefahrenfelder = Domänen eingeteilt.

Es sind dies:

- Gefahrenfeld Gas I: Gefahren an der Schnittstelle Steuerungs-und Kontrollsysteme (SCADA) innerhalb einer Organisation. Domäne: Betriebsführung und Infrastruktur.
- Gefahrenfeld Gas II: Gefahren an der Schnittstelle Steuerungs-und Kontrollsysteme (SCADA) zwischen verschiedenen Organisationen in Domäne: Infrastruktur.
- Gefahrenfeld Gas III: Gefahren, die sich aus Back-Office-Systemen („NICHT SCADA") ableiten lassen - innerhalb einer Organisation Domäne: Infrastruktur und Betriebsführung.
- Gefahrenfeld Gas IV: Gefahren, die sich aus der Kommunikation (z. B. Fahrplanmanagement) zwischen Unternehmen ableiten lassen („NICHT SCADA") Domäne: Infrastruktur, Betriebsführung, Energiehandel und Regulation.
- Gefahrenfeld Gas V: Gefahren, die sich aus Schnittstellen zwischen Steuerungssystemen (SCADA) und Verwaltungs- und Administrationssystemen innerhalb eines Unternehmens ableiten lassen. Domäne: Betriebsführung, Infrastruktur.
- Gefahrenfeld Gas VI: Gefahren, die sich aus Schnittstellen am Smart Meter bzw. im Smart-Meter-Netzwerk ableiten lassen. Domäne: Betriebsführung, Infrastruktur und Verbrauch.
- Gefahrenfeld Gas VII: Gefahren, die sich aus der Nutzung von Kunden HAN/BAN/NAN Netzwerken ableiten lassen. Domäne: Verbrauch.
- Gefahrenfeld Gas VIII: Gefahren, die sich aus der Nutzung externer Systeme („NICHT SCADA") ableiten lassen, die eine "direkte" Beziehung zum Verbraucher haben. Domäne: Betriebsführung, Verbrauch und Service Provider.
- Gefahrenfeld Gas IX: Gefahren, die sich aus Service- und Wartungs-Entwicklungsschnittstellen ableiten lassen – innerhalb eines Unternehmens. Domäne: Infrastruktur, Betriebsführung und Verbrauch.
- Gefahrenfeld Gas X: Gefahren, die sich aus der Nutzung von Decision-Support-Systemen ableiten lassen. Domäne: Betriebsführung.
- Gefahrenfeld Gas XI: Gefahren, die sich aus der Nutzung von Netzwerküberwachung und Securitymonitoring-Systemen ableiten lassen. Domäne: Infrastruktur, Betriebsführung und Service Provider.
- Gefahrenfeld Gas XII: Gefahren, die sich aus der Nutzung (zentral) europäischer Datenaustauschplattformen ableiten lassen. Domäne: Betriebsführung, Verbrauch und Service Provider.

4.3 Aufbau des Gefahrenkatalogs

Aus der Evaluation der Kommunikationsbeziehungen wurden die bereits identifizierten 226 Gefahren bestätigt. Der Gefahrenkatalog ist für alle Gefahrenfelder gleich aufgebaut. Er gliedert sich wie folgt:

Nr	Gefahrenkatalog gesamt	Gefahrenfelder														
Nr.	**Gefahrenbeschreibung**	**I**	**II**	**III**	**IV**	**V**	**VI**	**VII**	**VIII**	**IX**	**X**	**XI**	**XII**	**XIII**	**XIV**	**XV**
G 58	Gefahr von menschl. Fehlleistungen mit Auswirkungen	**G**	**G**	**G**	**G**	**G**		**G**	**G**	**G**	**G**	**G**	**G**			
G 59	organisatorische Defizite z. B. Ablauf von Zertifikaten			**G**			**G**			**G**						
S 02	Gefahr, dass Unbefugte Zugang zu nicht privilegierten Remote-Access-Accounts, LAN-Accounts mit Privilegien oder Remote- Access- LAN- Accounts mit Privilegien erhalten	S	S	S	S	S	S		S	S	S	S	S		S	S

Tabelle 1: Aufbau des Gefahrenkatalogs

Die laufenden Nummern haben ein G oder S vorangestellt. G steht für Gas und S steht für die Zuordnung zum Strom.

Teil III Ergebnisse der Risikoidentifikation

5. Grundlage der Risikobewertungen

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

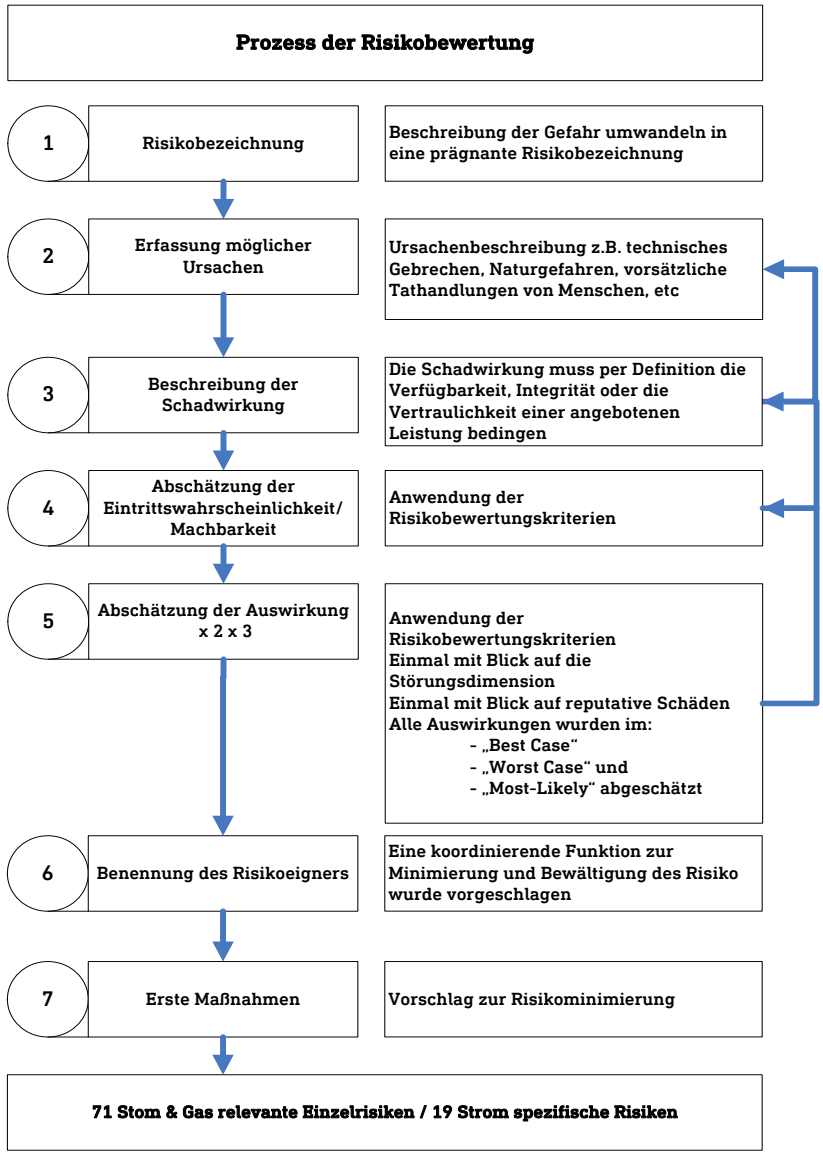
5.1 Allgemeines zur Herleitung der Bewertungskriterien

Die Bewertungskriterien wurden in mehreren Schritten erarbeitet. Um eine Abstufung mit Blick auf eine Risikoverteilung zu ermöglichen, müssen sowohl die Eintrittswahrscheinlichkeiten von Gefahren als auch deren Auswirkungsdimensionen auf die Versorgungssicherheit in Stufen beschrieben werden. Grenzwerte über die Festlegung von Vorfällen mit beträchtlichen Auswirkungen auf die Versorgungssicherheit wurden bis dato nur isoliert für Strom und Gas getrennt betrachtet. Für die Risikobetrachtungen ist es wichtig darzustellen, dass es einer skalierbaren und damit einer für alle Netzbetreiber, Erzeuger und Speicherbetreiber gleich gewichteten Abstufung bedarf, damit die Risiken in Relation für alle Organisationsgrößen gleich verteilt sind. Analog zum Bild der Sicherheitskette, wo immer das schwächste Glied die gesamte Stärke der Kette determiniert, wurde nach einer Bewertungsmetrik gesucht, die sowohl für ganz kleine Organisationen anwendbar ist als auch bei den großen bis sehr großen Organisationen sinnvoll eingesetzt werden kann. Um dieser Aufgabenstellung gerecht zu werden, wurde in einem zweiten Schritt nach einer flexiblen und für alle „Betreiber" allgemein gültigen Festlegung für die Bewertungen von Gefahren gesucht. Dazu wurden folgende Rahmenbedingungen formuliert:

- Für das Bewertungskriterium „Eintrittswahrscheinlichkeit" soll eine für alle „Betreiber"[3] 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 bzw. kriminellen Handlungen" entsprechend Rechnung tragen zu können.
- Für das Bewertungskriterium „Auswirkung" soll eine für alle Betreiber einheitliche Definition und Abstufung gefunden werden, die jedoch die spezifischen Versorgungsaufgaben bzw. Gegebenheiten der einzelnen Betreiber in absoluten Zahlen und unterschiedlichen Dimensionen berücksichtigt.
- In Summe soll die Relation der verschiedenen IKT-Risiken zueinander eine 1:1 Vergleichbarkeit zwischen den unterschiedlichen „Betreibern" ermöglichen. Damit soll auch eine individuelle Fortschreibung des Identifikations- und Bewertungsprozesses von Risiken bei allen „Betreibern" gewährleistet werden.

[3] TELKO und ISPs

5.2 Risikobewertungsprozess – Übersicht



Die in der Version 3.0-2018 identifizierten 69 Einzelrisiken wurden in einem ersten Schritt evaluiert.

In Summen wurde 226 Gefahren in mehreren Arbeitsworkshops zu 71 Risiken zusammengestellt.

Auch die rein stromspezifischen Risiken wurden evaluiert.

Abbildung 6: Risikobewertungsprozess

6. Ergebnisdarstellung der Einzelrisiken

6.1 Allgemeines

Die Risikoerfassung und die Aufbereitung der Ergebnisse werden hier kurz beschrieben:

A	B	C	D	E	F	G	H
Nr	**Risikobezeichnung**	**Ursachen**	**Wirkung**	**Wahr-scheinlichkeit**	**Höhe der Auswirkung**	**Risiko von**	**Risiko bis**
1	Risikobeschreibung	Mögliche Ursache, z. B. techn. Defekt	im Worst Case erhebliche Betriebsstörung bis hin zum Komplettausfall	4	1 - 5	4	20

Tabelle 2: Teil 1 der Einzelrisikoerfassungstabelle

Fortsetzung der Tabelle (1)

I	J	K	L	M	N	O
Risiko-Owner	**Schadens-ausmaß (€) VON**	**Schadens-ausmaß (€) ERWARTUNGS-WERT**	**Schadens-ausmaß (€) BIS**	**Maßnahmen zur Risikobewältigung**	**Anmerkungen; Maßnahmenvor-schläge**	**Kategorie**
NB	1	2	3	ISMS-insbesondere Zugriffskontrolle	G-Ref. 40, G-Ref. 64, G-Ref. 6, G-Ref. 7	organisatorische Sicherheit

Tabelle 3: Teil 2 der Einzelrisikoerfassungstabelle

Fortsetzung der Tabelle (2)

P	Q	R	S
ISO 27.002	**Gültigkeit bis (TT.MM.YY)**	**KK**	**NIS**
7,9,10	01.11.22	G, K	3

Tabelle 4: Teil 3 der Einzelrisikoerfassungstabelle

- Spalte A, laufenden Nummer – Entwicklungsnummer, losgelöst von der Risikohöhe
- Spalte B, Risikobezeichnung
- Spalte C, Kurzbeschreibung der möglichen Ursache
- Spalte D, Beschreibung der Auswirkung
- Spalte E, Bewertung der Eintrittswahrscheinlichkeit nach den Bewertungskriterien (hier können auch Intervalle eingetragen werden z. B. 1-2 gleichbedeutend für einmal

in 50 Jahren im „Best Case", im „Worst Case" kommt diese Gefahr einmal in 20 Jahren vor.

- Spalte F, Bewertung der Auswirkungsdimension nach den Bewertungskriterien (auch hier können Intervalle angegeben werden, z. B 1-5, gleichbedeutend einem Ereignis mit geringer bis katastrophaler Auswirkung im Worst Case).
- Spalte G, stellt das Risiko im „Best Case" dar, daher das Produkt aus Eintrittswahrscheinlichkeit und Auswirkung aus den niedrigsten Punkten in E und F.
- Spalte H, stellt das Risiko im „Worst Case" dar, daher das Produkt aus den höchsten Werten in den Spalten E und F. Der Erwartungswert „Most-Likely"-Fall definiert sich als arithmetisches Mittel aus den beiden Spalten G und H.
- Spalte I, definiert den Risikoeigner. Der Risikoeigner nimmt sich **koordinativ** der Bewältigung dieses Risikos in situ oder mit Blick auf die Prävention der risiko- minimierenden Maßnahmen an. (Dies hat immer nur empfehlenden Charakter).
- Spalte J, stellt eine erste Abschätzung des reputativen Impacts im „Best-Case"-Fall dar.
- Spalte K, stellt eine erste Abschätzung des reputativen Impacts im „Most-Likely"-Fall dar.
- Spalte L, stellt eine erste Abschätzung des reputativen Impacts im „Worst-Case"-Fall dar.
- Spalte M, beschreibt entweder direkt Maßnahmen zur Risikominderung oder gibt Empfehlungen wie z. B. die Implementierung eines ISMS.
- Spalte N, verweist auf die Gefahrennummer im Gefahrenkatalog.
- Spalte O, ordnet das Risiko einer Risikokategorie zu.
- Spalte P, Zuordnung zu den ISO 27.002 Controls.
- Spalte Q, Gültigkeitsdauer.
- Spalte R, KK, Wird dieses Risiko einem gemeinsamen Risiko TELKO-Energiewirtschaft zugordnet = G, Kann man daraus eine Kaskade ableiten, K.
- Spalte S, Zuordnung zum NIS-Kapitel des Fact-Sheets-Mindestsicherheitsstandard.

6.2 Risikoverteilung der Einzelrisiken im „Worst Case“

Bei Betrachtung des Worst-Case-Falls ergibt sich eine plausible Verteilung der Einzelrisiken zwischen hohen und geringen Risiken wie folgt:

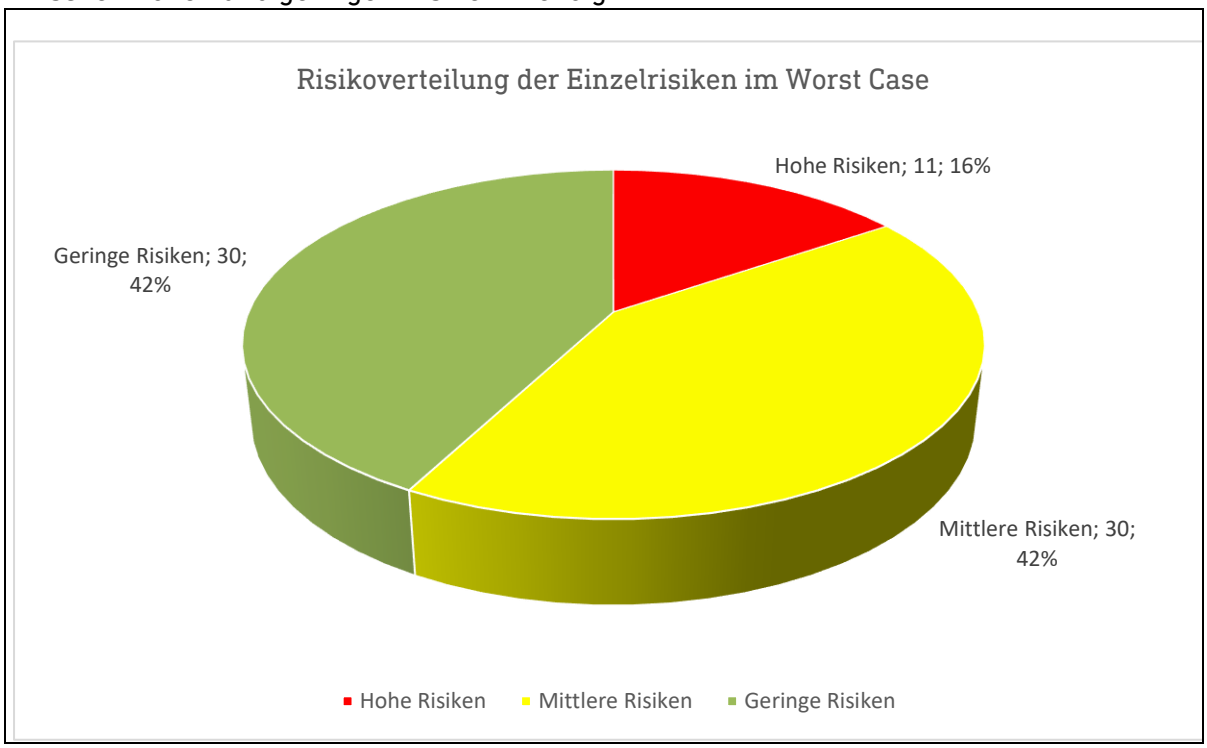


Abbildung 7: Risikoverteilung der Einzelrisiken im „Worst Case“

16 % hohe Risiken und gleichverteilt mit jeweils 42% mittlere Risiken und geringe Risiken stellen ein gewohntes Bild der Risikoverteilung dar.

7. Ergebnisdarstellung der Aggregationsrisiken

7.1 Aggregationsprozess

Die 71 Einzelrisiken wurden aus dem Gefahrenkatalog abgeleitet. Um die Einzelrisiken auf ein überschaubares Maß zu reduzieren, wurden die Einzelrisiken in Risikokategorien eingeordnet. Es wurden folgende 9 Risikokategorien definiert:

- Design und Architektur
- Eskalation und Kommunikation
- Hard- und Software
- Faktor Mensch
- Naturgefahr
- Normung und Recht
- Organisatorische Sicherheit
- Planung und Beschaffung
- Zugriffskontrolle und Krypto

Diese Kategorisierung wurde in einem ersten Schritt dazu benutzt, die Aggregation zu strukturieren. Es stellt jedoch nicht das alleinige Kriterium dar. Vielmehr wurde thematisch strukturiert aggregiert. Dies wurde in einem iterativen Prozess noch nach folgenden Gesichtspunkten bzw. Analysen zusammengefasst:

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

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 wurden ein Risikoeigner formuliert und Maßnahmen zur Risikominimierung als Vorschlag erarbeitet.

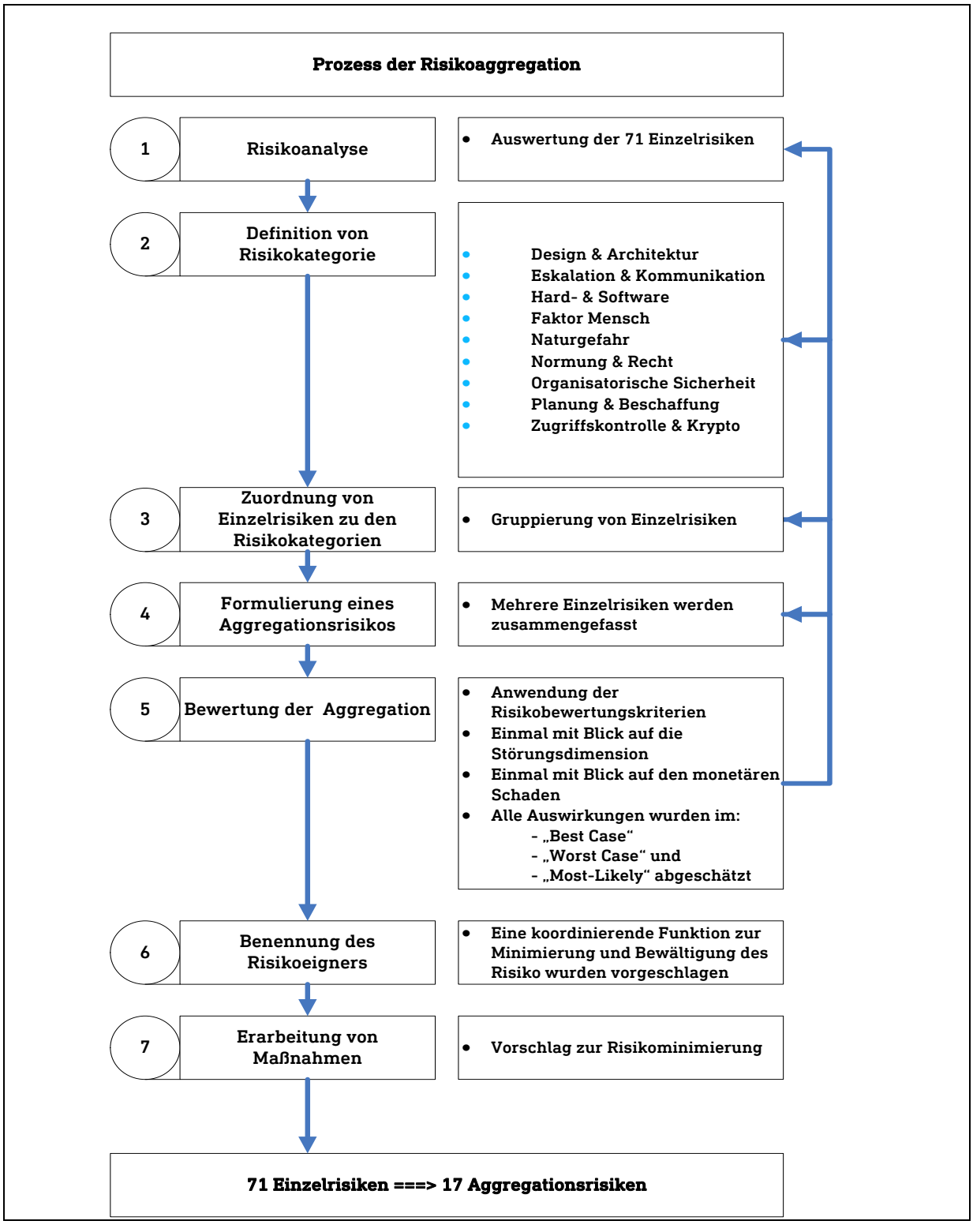


Abbildung 8: Risikoaggregationsprozess

7.2 Auswertung der Risikokategorien

Abbildung 9: Darstellung der Verteilung der Risikokategorien

8. Gegenüberstellung der Veränderungen bei den Aggregationsrisiken

Im Wesentlichen gibt es folgende große Änderungen bei den Aggregationsrisiken:

- Das Aggregationsrisiko 17 ist neu hinzugekommen und fasst die Aspekte der Zugriffskontrolle und Herausforderungen bei Einsatz kryptographischer Verfahren zusammen. Der Schutz von Vertraulichkeit und Integrität wird dabei auch den Herausforderungen bei der betrieblichen Implementierung gegenübergestellt.
- Außer bei den Risiken 1-3 wurden die Aggregationsbestandteile zum Teil erheblich umgruppiert.
- Die Risikohöhe im Worst Case wurde bei den Risiken 10 und 15 angepasst.

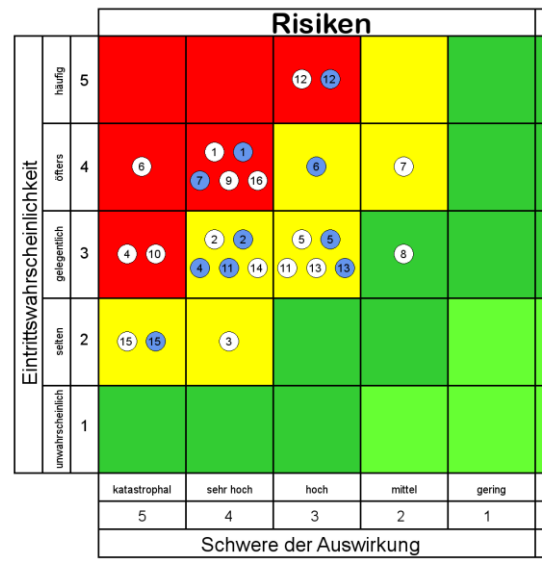


Abbildung 10: Aggregationsrisiken V3.0-2018

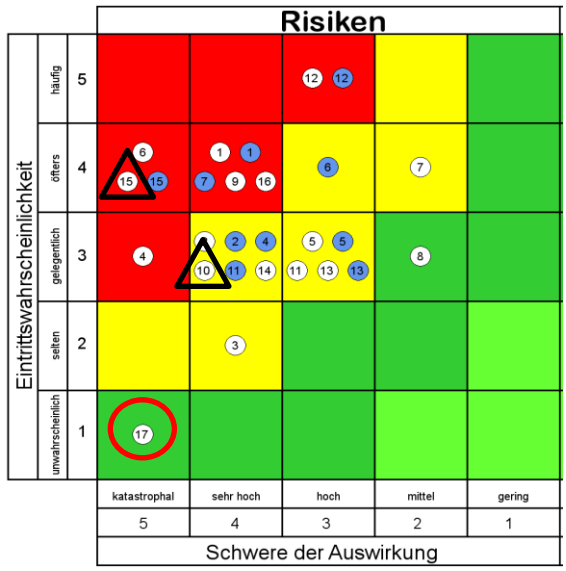


Abbildung 11: Aggregationsrisiken V4.0-2020

Neues Risiko Veränderte Risiken

9. Zusammenstellung der Ergebnisse aus dem Workshop mit der Telekommunikationswirtschaft

9.1 Allgemeines

Sowohl die Energiewirtschaft als auch die Telekommunikationsbranche haben im Vorfeld des ersten Informationsaustausches auf Ebene des jeweiligen Branchen-Expertenkreises eine Auswahl an Einzelrisiken, die Aggregationsrisiken sowie ein Exzerpt der Maßnahmen der jeweils anderen Branche zur Verfügung gestellt. Um ein gemeinsames Verständnis für die jeweiligen Risikobetrachtungen zu schaffen, wurden in einem ersten Schritt die jeweiligen Risikokriterien einander gegenübergestellt.
Seitens der Telekommunikationsbranche wurden 39 vorausgewählte Einzelrisiken, die einen Bezug zur Energiewirtschaft haben könnten, detailliert dargestellt.
Seitens der Energiewirtschaft wurden 16 vorausgewählte Einzelrisiken, die einen Bezug zur Telekommunikationsbranche haben könnten, detaillierter dargestellt.
Es existieren jedoch noch weitere „übereinstimmende" Risiken. Im Ergebnis der bis dato durchgeführten gemeinsamen **Workshops** unter Beteiligung von Energie- und Telekommunikationsbranche wurden zwei „Klassen" an Einzelrisiken definiert:

- G = Gemeinsames Risiko
- K = Kaskadenrisiko

Man kann die Erkenntnisse wie folgt zusammenfassen:

- Technische Gebrechen wie eine Leitungsunterbrechung bei vermeintlichen Redundanzen, die jedoch physisch eng beieinanderliegen, können zu Kaskaden führen.
- Ein Stromausfall kann einerseits infolge der beschriebenen Szenarien auftreten, stellt aber auch allein eine entsprechende Herausforderung dar. Die Stromausfallszeiten sollten in einer eigenen Diskussionsrunde harmonisiert werden.
- Ausfall von Services und Dienstleistungen, sei er durch kriminelles Verhalten initiiert oder technisch-organisatorischer Natur, stellt einen wesentlichen negativen Aspekt möglicher Fehlerfortpflanzungen dar bzw. kann amplifizierende Schadwirkungen nach sich ziehen.
- Der wahrscheinlich am schwierigsten zu beherrschende Effekt ist der Umgang mit neuen Technologien. Hier wird einerseits sehr oft an neue Netztechnologien wie bspw. das 5G-Netz gedacht. Mangelnde Cybersecurity bei IoT-Devices könnte indirekt wieder Stromausfälle nach sich ziehen. Aber auch neue gesetzliche Rahmenbedingungen wie z. B. die Förderung der Stromerzeugung durch erneuerbare Energien, die in weiterer Folge einen deutlich erhöhten Mess- und Regelaufwand bedeutet, stellen neue, bis dato wenig bewertbare Kaskadenpotentiale dar.
- Kaskaden in Richtung Zeitsynchronisation können für den Handel und den Marktzugang ein Problem darstellen.

- Fehlender Informationsaustausch/BCM-Reife/Anforderungen an den Informationsbedarf der jeweils anderen Branche könnten in Zukunft auch mögliche Effekte mit Sekundärwirkungen auf die jeweils andere Branche nach sich ziehen. Daher wird empfohlen, dass das Austrian Energy CERT (AEC) bei entsprechenden Schadereignissen die TK-Branche mit einbindet.
- Kaskaden, die durch die vermehrte Nutzung von Clouddiensten entstehen, ziehen die klare Empfehlung nach sich, für die Versorgungssicherheit eigene Infrastrukturen vorzuhalten.

Teil IV Maßnahmen & Empfehlungen

10. Empfehlungen

In der Version 3.0-2018 der IKT-Risikoanalyse wurden 36 Empfehlungen formuliert. Davon gelten 10 Maßnahmen, zumindest bei den als Betreibern wesentlicher Dienste gemäß NISV Organisationen, als bereits umgesetzt.
Die Empfehlungen leiten sich aus mehreren Perspektiven ab und fassen die Ergebnisse der Diskussionen aus den Expertenworkshops in den beiden Jahren 2019-2020 zusammen. Die Empfehlungen stellen daher einerseits die Auswertungsergebnisse der gesamten Risikoanalyse zusammen und bilden andererseits aus technischer Sicht den kleinsten gemeinsamen Nenner für möglichst alle in der Branche vertretenen Stakeholder. Es werden daher:

- die unmittelbaren Maßnahmen zur Risikominderung aus der Bewertung der Einzelrisiken zusammengestellt,
- die unmittelbar ausformulierten Maßnahmen aus der Bewertung der Aggregationsrisiken mitberücksichtigt,

die für die Branche wichtigsten Entwicklungen aus einer übergeordneten Sicht diskutiert und zugeordnet.

Die verschiedenen Empfehlungen haben selbstverständlich unterschiedlichste Adressaten. Tendenziell sind die Maßnahmen, die den Einzelrisiken zugeordnet wurden, auch durch die Unternehmen und Organisation selbst umzusetzen bzw. es sind diese bereits umgesetzt. Als Risiko per se persistieren sie dennoch und wurden genau aus diesem Aspekt heraus auch mit in die Risikoanalyse aufgenommen.
Die Maßnahmen, die sich in den Aggregationen wiederfinden, adressieren sowohl inter- als auch intraorganisatorische Empfehlungen. Die nachfolgende Zusammenstellung an Empfehlungen versucht daher die Schnittstellen zwischen interorganisatorischen Aspekten und Anregungen, die für die gesamte Branche relevant sind, aufzuzeigen. Viele Maßnahmen können bzw. sollen nur in der Gemeinsamkeit unter Beteiligung vieler Unternehmen umgesetzt werden.

10.1 Relevanz der Empfehlungen & Stakeholder

In der nachfolgenden Zusammenstellung der Empfehlungen wird in einem ersten Ansatz zwischen:

- Kritischen Infrastrukturbetreibern (KIs)
- Systemrelevanten Betreibern (Kurzbezeichnung „SysB“) und
- Behörden & Sonstige unterschieden

Die Gruppe der Unternehmen und Organisationen, die den Kritischen Infrastrukturen (KIs) zugeordnet werden können, lässt sich wie folgt beschreiben. Es werden Unternehmen in Österreich als „strategisch wichtige Unternehmen gemäß APCIP (vgl. dazu Kapitel 2.3.2)“, die kritische Infrastrukturen für Österreich betreiben, geführt. Diese Gruppe von Unternehmen /

Organisationen werden im Sinne der hier vorliegenden Einteilung als KIs verstanden. Diese wurden seitens BMI/BKA bereits via Information an die Geschäftsleitung über ihren Status informiert bzw. werden laufend informiert. Parallel dazu bzw. kongruent dazu sind dies Unternehmen, die gemäß NISV als Betreiber Wesentlicher Dienste einen Bescheid zugestellt bekommen haben. Behörden sind per Definition eine „Kritische Infrastruktur" in Österreich.
Die Kriterien für diejenigen Unternehmen, die der Gruppe der relevanten Systembetreiber zugeordnet wurden, werden in Abgrenzung zu den KIs bzw. Betreiber Wesentlicher Dienste gem. NISV in der Expertengruppe des PPD-Prozesses (PPD-AG) bzw. des PPD-BEI definiert.
Empfehlungen an die relevanten Betreiber (SysB) richten sich selbstverständlich auch an die Kritischen Infrastrukturen bzw. Betreiber Wesentlicher Dienste.
Im Rahmen der Empfehlungen werden auch Prozesseigner definiert. Unter Prozesseigner im Sinne der Empfehlungen werden Organisationen verstanden, die die Umsetzung der Empfehlungen **federführend koordinieren** sollen.
Von den Prozesseignern wird erwartet, dass diese im Rahmen einer periodischen Revision der Umsetzung der Empfehlungen bzw. der Risikoanalyse selbst dem Lenkungsausschuss (PPD-BEI) der Branchenrisikoanalyse den Umsetzungsstand darstellen und Anpassungen vorschlagen.

10.2 Priorisierung und Zeithorizonte der Empfehlungen

Im Rahmen der Abstimmungsarbeiten zum Bericht wurde vereinbart, dass es Empfehlungen zu Umsetzungszeiträumen geben soll. Es wurden daher drei Prioritäten (1-3) definiert, wobei 1 die höchste Priorität darstellt:

Für die Abstufung der Empfehlungen sind drei Prioritäten definiert worden:

- Priorität 1, kurzfristig (voraussichtlich bis 2 Jahre[4]), spätestens bis Ende 2022
- Priorität 2, mittelfristig (voraussichtlich 2-5 Jahre), spätestens bis Ende 2025
- Priorität 3, langfristige Umsetzung (voraussichtlich >5 Jahre) frühestens ab 2026

Die Empfehlungen wurden, dort wo sinnvoll, auch mit einer ersten Aufwandsschätzung versehen.

Alle bis dato erfassten Maßnahmenempfehlungen wurden seitens Oesterreichs Energie (OE) den zuständigen Arbeitskreisen zugeordnet und werden von dort aus einem Umsetzungskoordinationsprozess zugeführt. Eine analoge Vorgehensweise wird beim ÖVGW angestrebt.

[4] Ab Beginn der Umsetzung

10.3 Übersicht der Empfehlungen

Aus den 71 Einzelrisiken, 17 Aggregationsrisiken und den 19 stromspezifischen Einzelrisiken in 9 Risikokategorien wurden 27 Empfehlungen formuliert. Diese verteilen sich auf folgende Risikokategorien wie nachstehend abgebildet:

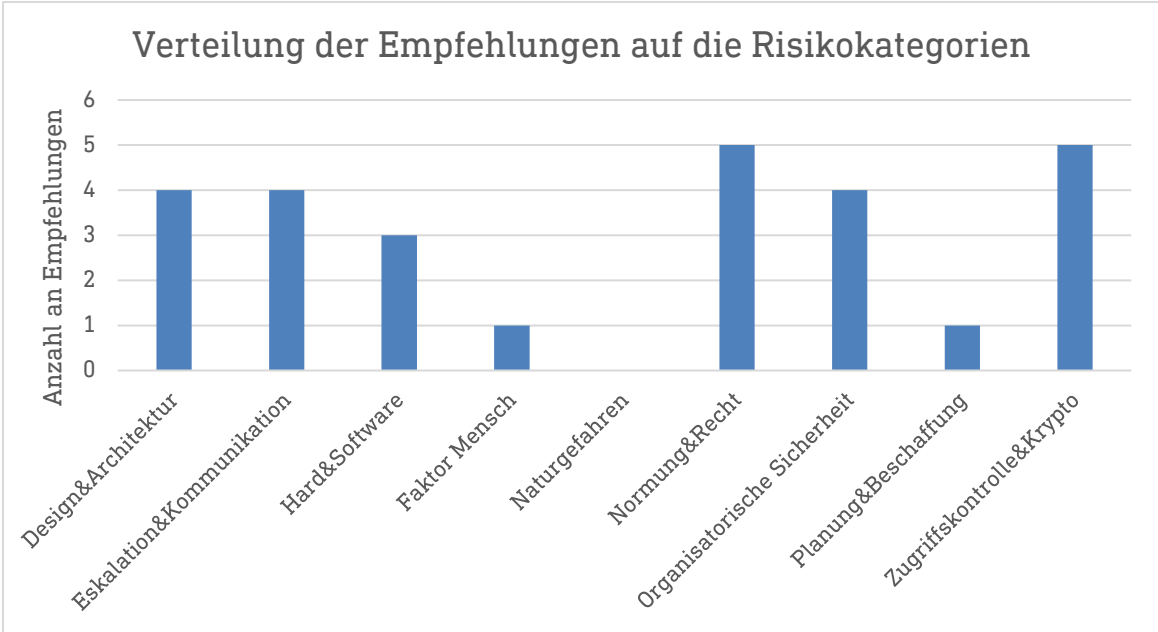


Abbildung 12: Verteilung der Empfehlungen auf die Risikokategorien

Abkürzungsverzeichnis

Abkürzung	Erklärung
AEC	Austrian Energy Cert
APCIP	Austrian Program Critical Infrastructure Protection
APCIP	Österreichisches Prorgamm zum Schutz kritischer Infrastrukturen
BAN	Border Area Network
BCM	Business Continuity Management
BKA	Bundeskanzleramt
BM.I	Bundesministerium für Inneres
BMK	Bundesministerium für Klimaschutz, Umwelt, Energie, Mobilität, Innovation und Technologie
BMLV	Bundesministerium für Landesverteidigung
BSI	Bundesam für Informationssicherheit in Deutschland
CERT	Computer Emergency Response Team
CIS	Customer Information System
CSP	Cybersecurity Plattform

Abkürzung	Erklärung
DA	Distribution Automatisation
DER	Distributed Energy Resources
ECA	E-Control Austria
EPCIP	European Program Critical Infrastructure Protection
EPCIP	Europäisches Programm „Schutz Kritischer Infrastrukturen“
HAN	Home Area Network
IKT	Informations- und Kommunikationstechnologie
IoT	Internet of Things Produkte
ISMS	Informationssicherheitsmanagementsystem
Intentionale Gefahren	Gem. ÖNorm S2401 werden darunter kriminelle Aktivitäten subsumiert
ISO	International abgestimmte Norm
ISP	Internetserviceprovider
IT	Infromationstechnologie
KI	Kritische Infrastrukturen
KVP	kontinuierlicher Verbesserungsprozess
LAN	Local Area Network
LSA	Lenkungsausschuss
NAN	Near-Area Network
NB	Netzbetreiber
NIS	Netz- und Informationssicherheit in der Union
NISB	NIS Behörde
NISG	NIS Gesetz,
NISV	NIS Verordnung
OE	Oesterreichs Energie
ONR	Österreichische Normenregel
OS	In der Regel Betriebssysteme
ÖSCS	Österreichische Strategie zur Cybersicherheit
ÖVGW	Fachverband Gas-Wärme
PPD	Private Public Dialog
PPD-AG	Expertenarbeitsgruppe
PPD-BEI	Beirat Cybersicherheit in dert Energiewirtschaft
QuaSte	Qualifizierte Stelle nach NISG
RTR	Rundfunk und Telekom Regulierungs-GmbH
SCADA	supervisory control and data acquisition
SPG	Sicherheitspolizeigesetz
SySB	Systemrelevante Betreiber
TELKO	Telekommunikationsprovider
TK	Telekommunikation
USV	Umfassende Sicherheitsvorsorge

Quellenverzeichnis

- Lit. ECA -01, BDEW-OE-White-Paper 2.0, Stand 05.2018, Anforderungen an sichere Steuerungs- und Telekommunikationssysteme Stand
- Lit.ECA-02, Netzsicherheit – Cybersicherheitsgesetz: https://www.rtr.at/de/inf/TKForum2016/Praesentation_NIS-Richtlinie_und_Netzsicherheit.pdf
- Lit.ECA-03, Zuordnungstabelle ISO 27001 sowie ISO 27002 und IT-Grundschutz: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Doku/Vergleich_ISO27001_GS.pdf?__blob=publicationFile
- Lit.ECA-04, Cyber-Risiken Österreich 2016: https://kuratorium-sicheres-oesterreich.at/wp-content/uploads/2017/09/KS%C3%96-Risikobericht-2016-Folder.pdf
- Lit.ECA-05, Report Cyber-Risikomatrix: https://kuratorium-sicheres-oesterreich.at/wp-content/uploads/2015/02/Cyberrisikoanalyse.pdf
- Lit.ECA-06, Critical Security Controls V6.0 CIS TOP 20: https://www.sans.org/media/critical-security-controls/critical-controls-poster-2016.pdf
- Lit.ECA-07, 7 Layers of OSI http://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-X.200-199407-I!!PDF-E&type=items
- Lit.ECA-08, Technische Sicherheitsanforderungen - Kompendium für technische Projektleiter und Entwickler: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/SOA/Management_Summary_Kompendium.pdf?__blob=publicationFile
- Lit.ECA-09, Bundesgesetz über die Organisation der Sicherheitsverwaltung und die Ausübung der Sicherheitspolizei (Sicherheitspolizeigesetz – SPG): https://www.jusline.at/gesetz/spg
- Lit.ECA-10, CYBER; Implementation of the Network and Information Security (NIS) Directive: http://www.etsi.org/deliver/etsi_tr/103400_103499/103456/01.01.01_60/tr_103456v010101p.pdf
- Lit.ECA-11, Cybersecurity Act https://sso.agc.gov.sg/Acts-Supp/9-2018/Published/20180312?DocDate=20180312
- Lit.ECA-12, RICHTLINIE DES EUROPÄISCHEN PARLAMENTS UND DES RATES über Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit in der Union (kurz NIS-Richtlinie) https://www.bundesanzeiger-verlag.de/fileadmin/Betrifft-Recht/Dokumente/externe%20dokumente/COM_2013__48_final.pdf
- Lit.ECA-13, Practical Overview of Implementing IEC 62443 Security Levels in Industrial Control Applications, Schneider Electric

» Lit.ECA-14, NISG, Bundesgesetz zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystemsicherheitsgesetz – NISG), https://www.ris.bka.gv.at/GeltendeFassung/Bundesnormen/20010536/NISG%2c%20Fassung%20vom%2021.10.2020.pdf

» Lit.ECA-15, Critical Security Controls V6.0 CIS TOP 20

» Lit.ECA-16, 7 Layers of OSI

» Lit.ECA-20, Bundesgesetz über die Organisation der Sicherheitsverwaltung und die Ausübung der Sicherheitspolizei (Sicherheitspolizeigesetz – SPG)

» Lit.ECA-21, RICHTLINIE DES EUROPÄISCHEN PARLAMENTS UND DES RATES über Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit in der Union (kurz NIS-Richtlinie)

» Lit.ECA-22, DIGITALSTRATEGIE DER EUROPÄISCHEN KOMMISSION, https://ec.europa.eu/info/sites/info/files/strategy/decision-making_process/documents/ec_digital-strategy_de.pdf

» Lit.ECA-23, NISV-Factsheets 08/2019, https://www.nis.gv.at/NIS_Fact_Sheet_8_2019_1.0.pdf

» Lit.ECA-24, Netz- und Informationssystemsicherheitsverordnung, NISV, https://www.ris.bka.gv.at/GeltendeFassung/Bundesnormen/20010536/NISV%2c%20Fassung%20vom%2021.10.2020.pdf

» Lit.ECA-25, Bericht Cybersicherheit 2020, https://www.bundeskanzleramt.gv.at/dam/jcr:d810f385-ed92-4aff-93a7-c67a4f56b02f/Cybersicherheit_2020.pdf, Fassung 25.01.2021