INFRA PROTECT

E-Control

Bericht

IKT-Risikoanalyse der Energiewirtschaft

Version 3.0

WHITE-VERSION

Auftraggeber:	Gesamtzahl Seiten:
E-Control	30
Aufgabensteller:	Anzahl Tabellen:
Dipl. Ing. Christian Schönbauer	02
Studienkennziffer:	Anzahl Abbildungen:
entfällt	12

Wien, 10.12.2018

Koordinierender Verfasser: DI Wolfgang Czerni, MBA

Management Summary

Im Jahr 2013 wurde ein Private-Public-Dialog (PPD) Prozess initiiert, der das Ziel verfolgt einen in der Branche abgestimmten Sicherheitsstandard für Risiken, die durch die Nutzung von Informations- und Kommunikationstechnologien (IKT) bedingt sind, zu definieren.
Dieser Sicherheitsstandard leistet einen entscheidenden Beitrag zur Umsetzung des künftigen NIS-Gesetzes und dessen Verordnungen. Dazu wurde ein Arbeitsgremium bestehend aus Vertretern der Ministerien BKA, BM.I, BMLV, BMNT, E-Control (ECA) sowie den Interessensvertretungen der Elektrizitäts- und Gaswirtschaft eingerichtet. Erweitert wurde das Gremium um das Austrian Energy CERT (AEC), das bereits als Umsetzung einer früheren Maßnahme von einer Arbeitsgemeinschaft aus Unternehmen der Elektrizitäts- und Gaswirtschaft gegründet wurde. Der Bericht fasst die Ergebnisse aller betrachteten Risiken der Elektrizitäts- und Gaswirtschaft zu einer Gesamtrisikobetrachtung zusammen. Der Gesamtrisikokatalog umfasst:

- Zugriffskontrolle und Kryptographie
- Design- und Architektur der IKT
- Eskalation und Kommunikation
- Hard- und Software
- Human Factors
- Naturgefahren
- Normung und Recht
- Organisatorische Sicherheit
- Planungs- und Beschaffungsprozesse in der IKT

Zur Risikoreduktion wurden Empfehlungen aus drei wesentlichen Blickwinkeln heraus abgeleitet.

Empfehlungen, die sich an die Unternehmensprozesse richten:

- Berücksichtigung aller zusammengestellter Risiken bei der Implementierung von betrieblichen Abläufen in der Organisation
- Sicherstellung eines funktionsfähigen Business Continuity- und Krisenmanagements, u. a. auch durch regelmäßige Teilnahme an Übungen sowie unter Einbindung des AEC
- Gewährleistung funktionaler Anforderungen unter Berücksichtigung entsprechender Sicherheitsmaßnahmen in allen Phasen des Produkt-Life-Cycles
- Umsetzung von Security Policies und einer Security-Organisation im Unternehmen (Beispiel: Stabstelle eines Informationssicherheitsbeauftragten oder CISO)

Empfehlungen zur Definition eines „Stand der Technik“ in der Umsetzung des Sicherheitsstandards:

- Umsetzung der ISO 27.001, ergänzt um die Branchennorm ISO 27.019 und der Empfehlungen des BDEW-OE-White-Papers sowie Prüfung der im Anhang aufgelisteten technischen Normen und Managementnormen
- Implementierung entsprechender Testregime, wiederkehrende Tests und Auditierungen von bestehenden und geplanten IKT-Systemen
- Intensivierung des organisationsübergreifenden Informations- und Erfahrungsaustausches zu konkreten Sicherheitsimplementierungen unter Einbindung des AECs

Empfehlungen für nationale und internationale Rahmenwerke:

- Einführung eines für die Branche relevanten Technologiefolgeabschätzungsprozesses unter frühzeitiger Einbindung des IKT-PPD-Cybersicherheitsbeirats Energiewirtschaft:
  - bei Einsatz neuer Technologien
  - bei neuen gesetzlich-normativen Regelungen
- Einforderung entsprechender organisatorischer und technischer Securitystandards bei Herstellern und Lieferanten
- Mitwirkung und Entsendung von Ressourcen zur Abstimmung und Harmonisierung von Sicherheitsstandards für IKT-Produkte und Dienstleistungen auf EU-Ebene
- Ein regelmäßiges Review der Risikoanalyse, der Domänenmodelle.at (Strom und Gas) und der Maßnahmenumsetzungen durch die IKT-PPD-Expertenarbeitsgruppe
- Mitgestaltung von Sicherheitsstandards im Rahmen der nationalen Umsetzung der NIS-Richtlinie (Mapping-Prozess) durch den IKT-PPD-Cybersicherheitsbeirat

Allen Risiken sowie Empfehlungen wurden Risikoeigner bzw. Adressaten zugeordnet. Systemrelevante Netzbetreiber, Erzeuger und Speicherbetreiber werden durch die NIS-Richtline im Rahmen der Identifikation der Betreiber wesentlicher Dienste festgelegt. Darüber hinaus wurde im Anhang eine Liste „relevanter“ Strom- und Gasnetzbetreiber, Erzeuger sowie Speicherbetreiber zusammengestellt, die in den gesamten PPD-Prozess mit einbezogen werden sollten.

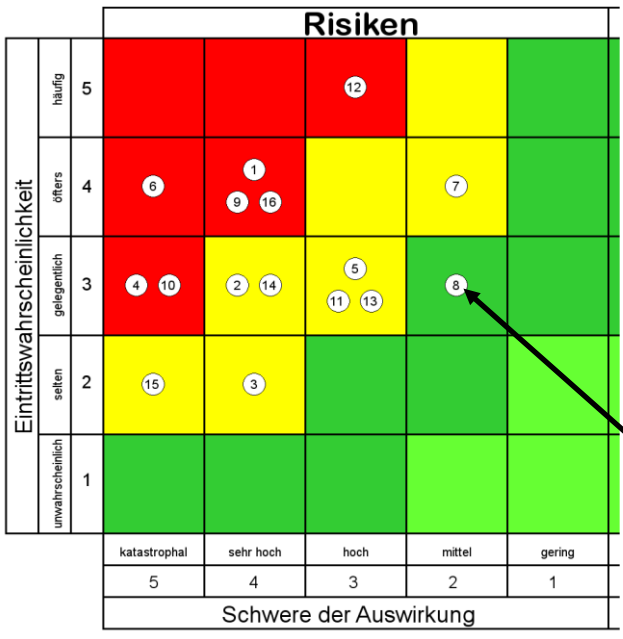
Kurzfassung

Der vorliegende Bericht fasst die Ergebnisse der Zusammenführung der beiden IKT-Risikoanalysen Strom und Gas im Zeitraum von Juli 2017 bis September 2018 zusammen. Im Wesentlichen werden vier Schwerpunkte beschrieben.
Im Teil I wird die Methodik und Vorgehensweise der Zusammenführung zu einer gemeinsamen Risikobetrachtung in der Energiewirtschaft vorgestellt.
Der Teil II beschäftigt sich mit der Aktualisierung der beiden Kommunikationsgeflechte im Strom und Gas und beschreibt den Versuch, diese zusammenzuführen. Zusätzlich wird der gesamte Gefahrenkatalog als Basis für den Teil III beschrieben.
Der Teil III widmet sich der Zusammenfassung der wesentlichen Ergebnisse des Risikoidentifikations- und Bewertungsprozesses. Die harmonisierten Risikobewertungskriterien, 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.
Teil IV beschäftigt sich mit den abgeleiteten übergeordneten Empfehlungen der Weiterentwicklung von Cybersicherheit für die Energiewirtschaft aus inter- und intraorganisatorischer Sicht. In Ergänzung zu den Empfehlungen, die sich aus den Maßnahmen zur Risikominimierung aller erkannter Risiken ableiten lassen, wird ein Private-Public-Dialog-Prozess beschrieben. Dieser soll die konzeptionellen Grundlagen für die Mitwirkung der Energiebranche an den vom Bundeskanzleramt festzulegenden Mindestsicherheitsstandards im Rahmen des künftigen NIS-Gesetzes darstellen. Das so koordinierte Zusammenwirken der Energiewirtschaft mit den Behörden soll sicherstellen, dass praxisgerechte und umsetzbare Durchführungsverordnungen seitens der NIS-Behörde vorgegeben und in weiterer Folge auch kontrolliert werden können.

In Summe wurden in elf Arbeitsworkshops 225 relevante Gefahren identifiziert. Diese wurden in weiterer Folge zu 69 gemeinsamen Einzelrisiken und weiteren 19 stromspezifischen Risiken anhand der festgelegten Risikobewertungskriterien nach verschiedenen Gesichtspunkten bewertet und analysiert. Die 69 gemeinsamen Einzelrisiken wurden in mehreren Iterationen zu 16 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 36 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 16 Aggregationsrisiken wurde der „Worst Case“ herangezogen. Es wurden 7 hohe Risiken, 8 mittlere Risiken und ein geringes Risiko bewertet. Nachfolgend wird exemplarisch die Aufbereitung der Ergebnisse 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.

Allen gemeinsam ist eine „Worst Case“ Betrachtung.

Abbildung 1: Worst Case Risiken

Eines der Risken beschäftigt sich mit der Unsicherheit im Umgang mit neuen Technologien, die im produktiven Betrieb unerwartete funktionale Störungen und/oder unerwartete Sicherheitslücken aufweisen können. Im Rahmen der Risikoanalyse Strom war der fehlende Technologiefolgeabschätzungsprozess eines der höchsten Risiken. Dieses Aggregationsrisiko adressiert gemeinsam mit anderen die Herausforderungen im Umgang mit neuen Technologien, beleuchtet aber auch die Problemstellungen, die sich durch die relativ lange Nutzungsdauer von „IKT-Komponenten und -Systemen“ in der Energiewirtschaft ergeben. Ein anderes Risiko beschreibt unvorhergesehene Dimensionen an Naturereignissen, die auch wesentlich durch den Klimawandel determiniert sein können. Ein weiteres Risiko diskutiert die Notwendigkeit einer professionellen Konzeption des Störungs-, Notfall- und Krisenmanagements und fordert andererseits ein entsprechendes Aus- und Fortbildungsprogramm im Business Continuity Management. Ein weiteres bereits identifiziertes Risiko von menschlichen Fehlleistungen fokussiert auf zwei Aspekte: Einmal der Faktor Mensch per se, der unter Stress zu Fehlleistungen neigt. Der zweite Punkt beschreibt eine gewollte oder ungewollte technische Schwachstelle, die vorsätzlich oder auch nur fahrlässig durch menschliche Handlungen ausgenutzt werden kann. Motiviert durch die Ereignisse um die Spectre & Meltdown Schwachstellen wurden solche Angriffsziele in einem weiteren Risiko zusammengefasst. Die Beschreibung einer der wesentlichsten Kaskaden zwischen Strom und Gas in der Energiewirtschaft determiniert ein definiertes Risiko, nämlich partieller Stromausfall für einen Zeitraum größer 48h. In einem weiteren Risiko wird das Spannungsfeld zwischen gesetzlichen Auflagen, die die Informationsbedürfnisse der Bevölkerung befriedigen sollen und Geheimhaltungserfordernissen nach dem Need-to-know-Prinzip, beschrieben. Zu jedem Einzel- und Aggregationsrisiko wurden Minimierungsmaßnahmen vorgeschlagen. Viele davon sind in den meisten Unternehmen bereits umgesetzt.

Die Ergebnisse wurden in einer großen Expertengruppe, bestehend aus Vertretern verschiedener Organisationsgrößen, 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 auch als Prozesseigner des gesamten Private-Public-Dialog-Prozesses.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Teil I Methodik und Kontext

1. Vorgehensweise und Aufbau der Risikoanalyse

Der vorliegende Bericht beschreibt in vier Teilen die grundsätzliche Vorgehensweise zur Zusammenführung der beiden IKT-Risikoanalysen Strom in der Version 2.0 und der Risikobetrachtung im Gas in der Version 1.0. Die Zusammenführung stellt dabei einen wesentlichen Teil der Weiterentwicklung und Implementierung eines kontinuierlichen Verbesserungsprozesses für bereits identifizierte bzw. latente Gefahren für die Informationssysteme in der Energiewirtschaft dar.
Der Bericht umfasst daher folgende Abschnitte:

- Teil I beschreibt die allgemeine Vorgehensweise der Zusammenführung
- Teil II stellt die Ergebnisse der Überarbeitung der beiden Domänenmodelle zusammen
- Teil III umfasst die Zusammenstellung von Einzel- und Aggregationsrisiken
- Teil IV fasst alle Empfehlungen zur Definition eines Mindestsicherheitsstandards zusammen und definiert einen Vorschlag für die Verbesserungsmöglichkeiten des Gesamtprozesses im Rahmen eines Private-Public-Dialogs (PPD).

Die grundsätzlichen Prozessschritte zur Risikoidentifikation und Bewertung wurden in den beiden Risikoanalysen Strom und Gas bereits eingehend beschrieben. Dieser Ablauf wurde beibehalten, wobei in der Ausgestaltung der einzelnen Arbeitsschritte der Kontext des Risikomanagementprozesses zu den Vorgaben der „controls“ der ISO 27.002:2013 und dem BDEW-White-Paper deutlicher hervorgehoben wird.

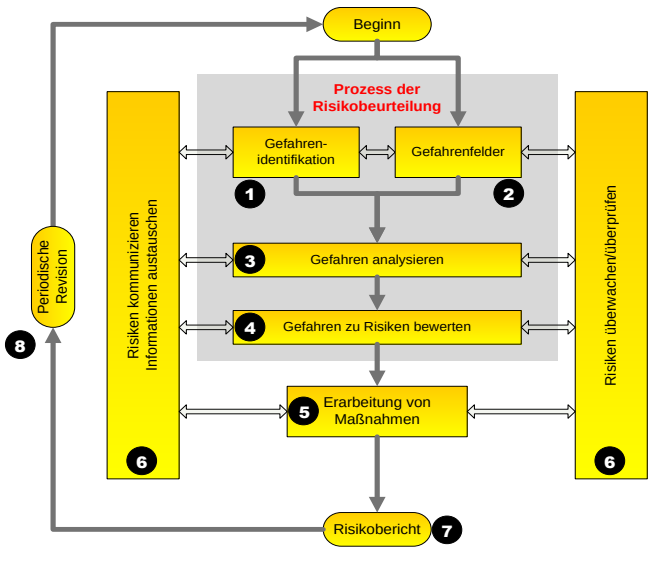


Abbildung 2: Vorgehensweise in der Risikoanalyse

Der Gefahrenidentifikations- und Bewertungsprozess von potentiellen Gefahren, die durch die Nutzung von Informations- und Kommunikations-technologien in der Energiewirtschaft bedingt sind, bezieht sich primär auf die nebenstehenden Prozessschritte 1-5. Die Vorgehensweise orientiert sich an den Vorgaben der „ISO 31.000 risk-management“ und an der „ONR 49.002-2, Risikomanagement für Organisationen und Systeme, Leitfaden für die Methoden der Risikobeurteilung“.

Der Prozess der Risikoidentifikation stellt mit Blick auf ein gesamtstaatliches Risikomanagement für die Risiken, die sich aus der Nutzung von Informations- und Kommunikationstechnologien (IKT) in der Energiewirtschaft lassen, nur den ersten Schritt dar.
Im Rahmen des Zusammenführungsprozesses wurden auch die normativ vorgesehenen Risikomanagementprozessschritte 6 und 8 (vgl. dazu Abbildung 2: Vorgehensweise in der

Risikoanalyse) diskutiert und in Form eines Vorschlags im Rahmen des PPD-Energiewirtschaft konkretisiert (siehe dazu Abschnitt 7, PPD-Prozess in der Energiewirtschaft).
Der **Teil II** beschreibt die Ergebnisse der Überarbeitungen der beiden Domänenmodelle Gas- und Strom als Basis für die Gefahrenidentifikation.
Im Teil III werden die Einzel- und Aggregationsrisiken nach der Zusammenführung aus den beiden Betrachtungen Strom und Gas zusammengestellt. Dabei wurde erkannt, dass es für die Elektrizitätswirtschaft residuale Risiken gibt, die den speziellen Gegebenheiten in der Stromversorgung geschuldet sind. Eine gemeinsame Betrachtung ist für diese Risiken nicht sinnvoll.
Die Ergebnisse bauen auf den beiden Risikoanalysen Strom und Gas jeweils mit Stand 10.01.2016 auf.
Der **Teil IV** beschäftigt sich mit der Festlegung von Mindestsicherheitsstandards, die als Basis für die „Auditierung“ durch qualifizierte Stellen im Rahmen der Verordnungsermächtigungen der NIS-Behörden herangezogen werden soll.
Das vorliegende Dokument stellt eine Zusammenfassung der Risikobetrachtungen dar, die zur Veröffentlichung freigegeben sind. Detaillierte Arbeitsergebnisse sind als TLP-AMBER („Vertraulich“) klassifiziert und nur den Mitgliedern der Arbeitsgruppe und den mitwirkenden Organisationen zugänglich.

2. Zielsetzungen und Kontext der Risikoanalyse

2.1 Allgemeines

Der vorliegende Bericht soll die Grundlagen für eine Risikoevaluation in der Energiewirtschaft schaffen. 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 die Kriterien für Informationssicherheit:

- 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 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.
Ziel dieses Prozesses ist es, die Mindestsicherheitsstandards in der Energiewirtschaft durch einen gemeinsamen Erarbeitungsprozess mit der künftigen NIS-Behörde abzustimmen und festzulegen. Im Rahmen der Erarbeitung der Grundlagen zum künftigen NIS-Gesetz wurden in Sektorgesprächen die Schwellenwerte für die Festlegung von Betreiber wesentlicher Dienste nach NIS-Richtlinie definiert. In diesem Zusammenhang wurde auch der Prozess der Festlegung von Mindestsicherheitsstandards und Meldeschwellen zu relevanten Sicherheitsvorfällen konkretisiert. Nach derzeitigem Wissensstand ist es geplant, Auditierungen von Sicherheitsstandards durch die NIS Behörden oder durch qualifizierte Stellen vorzunehmen. In diesem Kontext spielt der hier beschrittene PPD-Prozess eine wesentliche Rolle, da durch konkrete Festlegung von Maßnahmen de facto ein Branchensicherheitsstandard definiert werden kann. Unternehmen, die „wesentliche Dienste“ im Sinne des NIS-Gesetzes erbringen, werden durch einen Bescheid der NIS-Behörde identifiziert. Sie haben in der Folge die entsprechenden Nachweise zu erbringen und der Behörde vorzulegen.
Die Verordnungsermächtigung der NIS-Behörden umfasst daher die Festlegung von Grenzwerten der Meldepflicht und die Definition von Sicherheitsstandards.

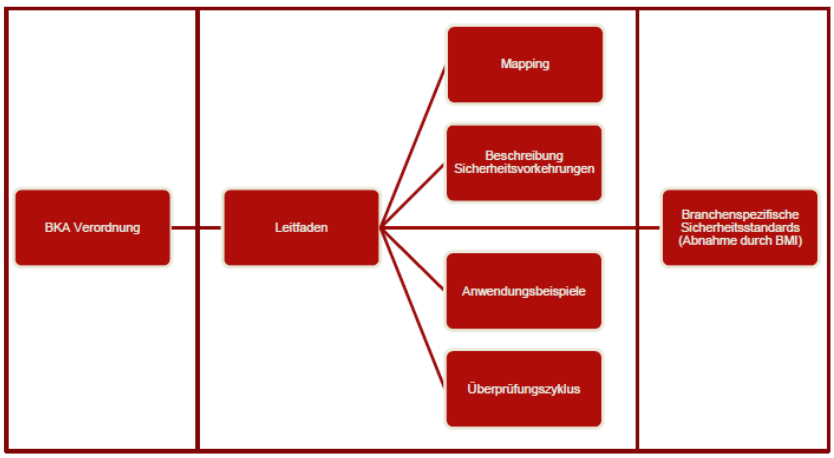


Abbildung 3: Konkretisierung der Mindestsicherheitsstandards seitens BKA-CSP

Die Ergebnisse der Risikoanalyse leisten daher einen Beitrag zum „Leitfaden“, dem „Mapping“, und der „Beschreibung der Sicherheits-vorkehrungen zur Festlegung von branchen-spezifischen Sicherheitsstandard, die durch die NIS-Behörde definiert wird.

	Sicherheitsmaßnahmen
1.	**Information Security Governance und Risikomanagement**
1.1.	Risikoanalyse
1.2.	Erstellung einer Informationssystemsicherheitsleitlinie
1.3.	Audits von Informationssystemen
1.4.	Kapazitäts- und Ressourcenmanagement
1.5.	Interne Audits
1.6.	Organisation und Personal
2.	**Ecosystem Management**
2.1	Steuerung, Überwachung und Überprüfung von Dienstleistern
2.2	Informationssicherheitsrichtlinie zu Dienstleistungsbeziehungen
3.	**Sicherheitsarchitektur**
3.1.	Systemkonfiguration
3.2	Netzwerksicherheit
3.3.	Asset Management
3.4.	Traffic filtering
3.5.	Kryptographie
4.	**IT-Security Administration**
4.1.	Administration Accounts
4.2.	Administration information systems

	Sicherheitsmaßnahmen
5.	**Identitäts- und Zugriffsmanagement**
5.1.	Authentifizierung und Identifizierung
5.2.	Zugriffsrechte
6.	**IT Security Maintenance**
6.1.	IT Security maintenance procedure
6.2.	Fernzugriff
7.	**Physische Sicherheit und die Sicherheit des Umfelds**
7.1.	Physische und umgebungsbedingte Sicherheit
8.	**Erkennung von Anomalien**
8.1.	Erkennung von Angriffen
8.2.	Logging
8.3.	Logs correlation und analysis
9.	**Bewältigung von Sicherheitsvorfällen**
9.1.	Vorfallsreaktionsplan
9.2.	Vorfallsbericht und Vorfallsmeldung
9.3.	Communication with competent authorities
9.4.	Vorfallsanalyse
10.	**Betriebskontinuität**
10.1.	Betriebskontinuitätsmanagement
10.2.	Notfallwiederherstellung
11.	**Krisenmanagement**

Um diesem Anspruch gerecht zu werden, wurden wesentliche Normen und Regelungen zusammengestellt. Diese Zusammenstellung wird mit der NIS-Behörde abzustimmen sein. Die konkreten Umsetzungen müssen durch die betroffenen Unternehmen intern evaluiert werden.

Abbildung 4: Struktur der der Mindestsicherheitsstandards seitens BKA-CSP

3. Wesentliche Arbeitsschritte der Zusammenführung

Im nachfolgenden Abschnitt werden die wesentlichsten Arbeitsschritte kurz zusammengefasst.

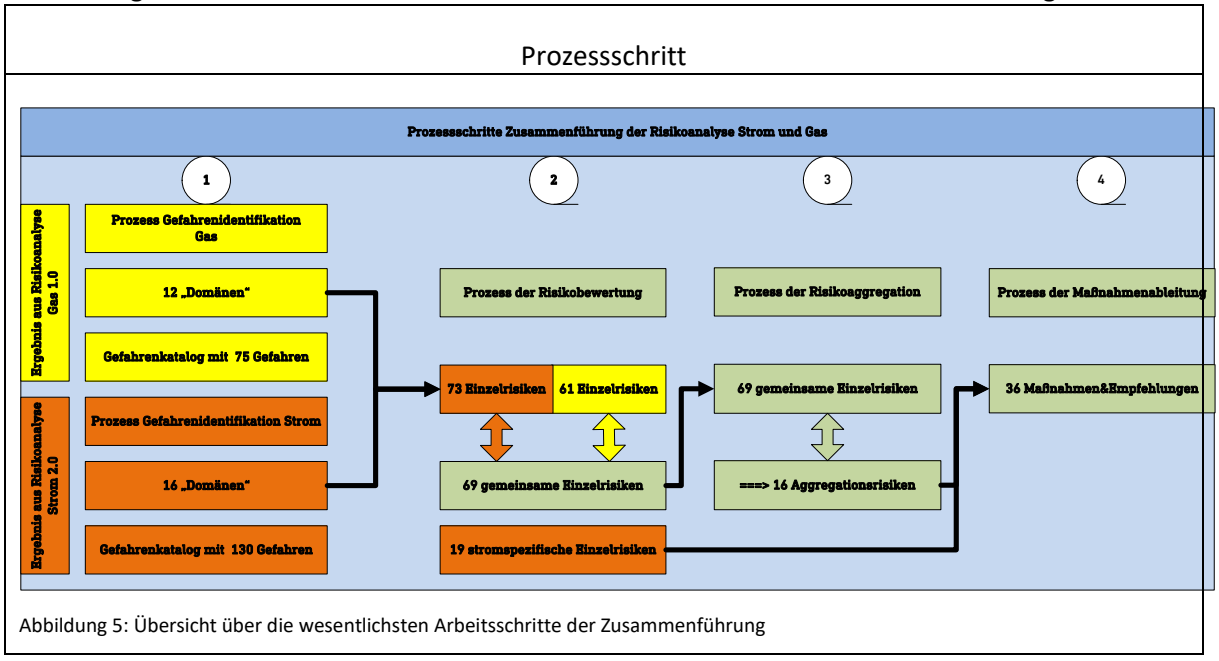


Abbildung 5: Übersicht über die wesentlichsten Arbeitsschritte der Zusammenführung

Der Prozessschritt 1, Gefahrenidentifikation wurde in zwei Arbeitsschritten abgearbeitet:

- Review des Domänenmodells
- Review und Aktualisierung möglicher Gefahren, die sich aus den Kommunikationsbeziehungen im Domänenmodell.at ableiten lassen

Der Prozessschritt 2, Risikobewertung, wurde in sechs Arbeitstakten durchgeführt:

- Überarbeitung bzw. Zusammenführung der Risikobewertungskriterien
- Zusammenführung der beiden Gefahrenkataloge
- Review und Aktualisierung der bestehenden Risikobewertungen anhand der Bestandsrisikomatrizen
- Ergänzung von bis dato nicht identifizierten Gefahren. Bewertung dieser zu Risiken, bzw. Ergänzung von Risikobezeichnung möglicher Ursachen sowie Anpassung der Auswirkungsdimension
- Zuordnung der Risiken zu den ISO 27.002 bzw. ISO 27.019 Controls
- Überarbeitung der Risikoeigner und Empfehlungen zur Risikominderung in den jeweiligen Einzelrisiken

Der Prozessschritt 3, Risikoaggregation, wurde in zwei Teilen bearbeitet:

- Neuaggregation der gemeinsamen Einzelrisiken
- Ergänzung und Anpassung der Aggregationsrisiken an die Veränderungen und Ergänzungen bei den Einzelrisiken

Der Prozessschritt 4, Empfehlungen, wurde in fünf Phasen eingeteilt:

- Review und Aktualisierung bzw. Durchsicht der bestehenden Maßnahmenformulierungen
- Identifikation des Sachstands der Umsetzung der empfohlenen Maßnahmen
- Konkretisierungen bzw. Anpassung und Ergänzungen der Empfehlungen
- Zuordnung der Empfehlungen zu den Aggregationsrisiken, um eine transparentere Herleitung der Maßnahmen sicherstellen zu können
- Zuordnung der Empfehlungen zu den Vorgaben des BDEW-Whitepapers

3.1 Prozessschritt 1, Gefahrenidentifikation

Der Prozessschritt 1, Gefahrenidentifikation, bestand im Wesentlichen daraus, die Kommunikationsbeziehungen auf Aktualität zu prüfen und neue bzw. bis dato nicht erkannte Gefahren in den Gefahrenkatalog einzuarbeiten.

Basierend auf den verschiedenen Kommunikationsgeflechten wurde auch der gesamte Gefahrenkatalog neu zusammengestellt.

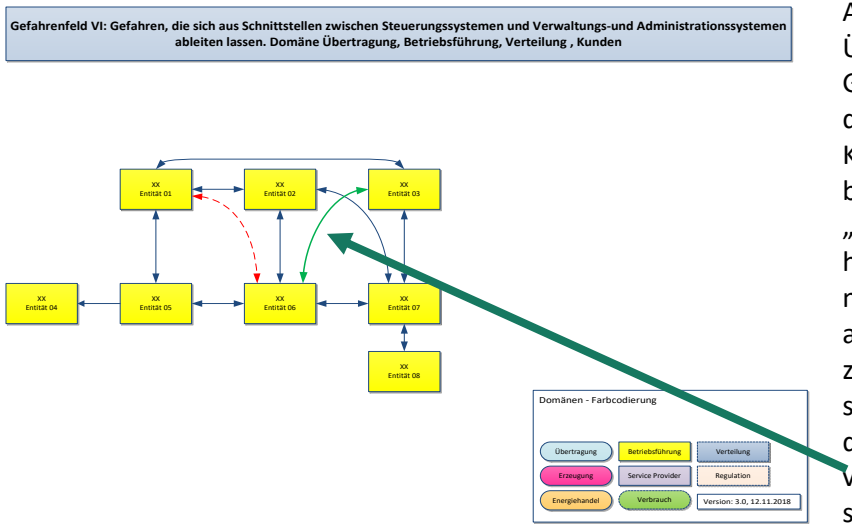


Abbildung 6: Kennzeichnung neu hinzugekommener Kommunikationsstrukturen

Als Basis für die Überarbeitung des Gefahrenkatalogs wurden die letztgültigen Kommunikations-beziehungen im „Domänenmodell.at“ herangezogen und an die neuesten Erkenntnisse angepasst. Rot gekenn-zeichnete Beziehungen stellen die Aktualisierungen der jeweiligen Vorgänger-version dar. In grüner Farbe sind die aktuell neu hinzugekommenen Kommunikationsbeziehungen gekennzeichnet.

Im Wesentlichen wurden die Kommunikationsbeziehungen, die sich aus der Nutzung von Elektronischen Datenaustausch Plattformen ergeben, ergänzt.
Im Strom-Domänenmodell wurden 16 verschiedene Kommunikationsgeflechte, im Gas-Domänenmodell wurden 12 verschiedene Kommunikationsgeflechte definiert.
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. In Summe wurden daher nur einige wenige Interdependenzen identifiziert. Die Abhängigkeit der Verfügbarkeit von Strom auf den Gasbetrieb versteht sich hier als selbstverständliche Kaskade.

Im Ergebnis wurden **226 Gefahren** zusammengestellt und ausgewertet.

3.2 Prozessschritt 2, Risikobewertung

In einem ersten Schritt wurden die Risikobewertungskriterien überarbeitet. Dieser Schritt determiniert im Wesentlichen die Gültigkeit der Ziele der Risikoanalyse. Im Rahmen dieses Prozesses werden die Abstufungen des „nennenswerten und flächendeckenden Stromausfalls“ bzw. die „nennenswerten Liefereinschränkungen im Gas“ definiert.

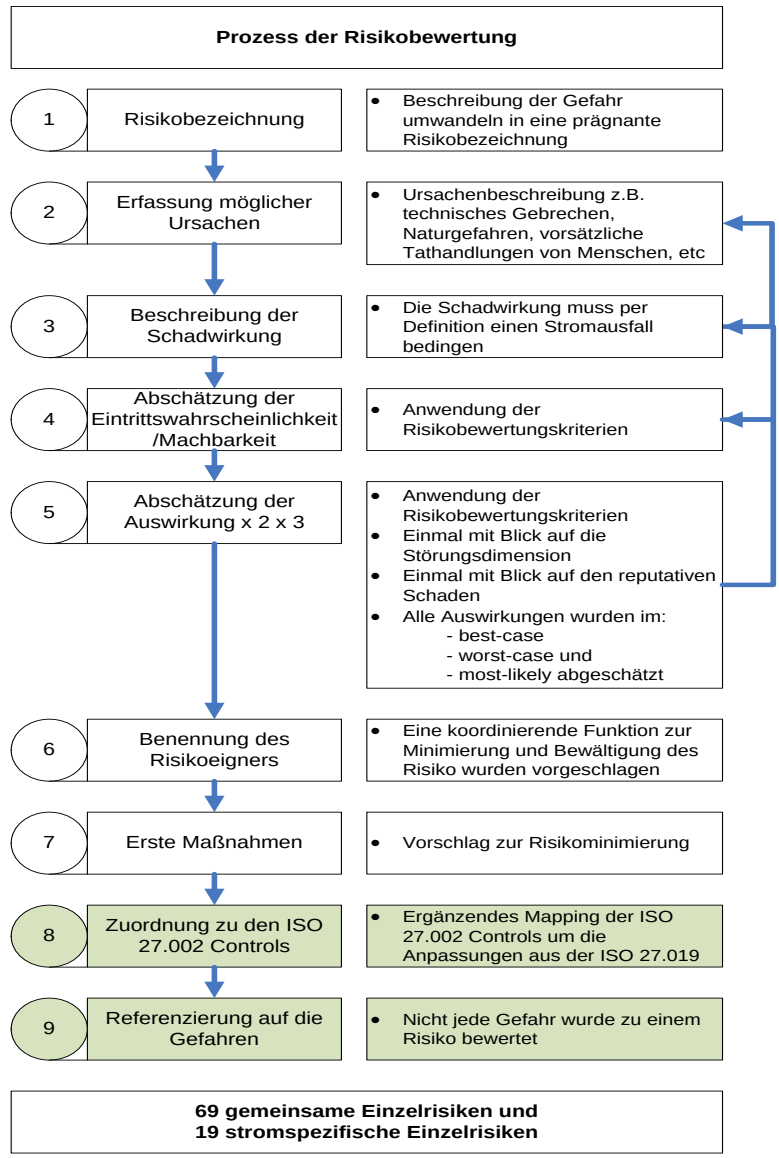


Abbildung 7: Anpassung des Risikobewertungsprozesses

Damit werden mögliche Auswirkungsdimensionen bei Störungen der IKT auf die Energieversorgung bzw. auf die Versorgungssicherheit insgesamt in einer festgelegten Abstufung beschrieben und festgelegt. Die Risikobewertungs-kriterien wurden entsprechend angepasst.
Der Prozess der Risikobewertung für bereits identifizierte Gefahren wurde jedoch insofern angepasst, als dass zusätzlich zu den bereits formulierten Risikominimierungs-empfehlungen auch die entsprechenden Controls aus der ISO 27.002 mit referenziert wurden.

Parallel dazu wurde die Gefahrennummer aus dem Gefahrenkatalog mit in die Risikoerfassung aufgenommen und festgehalten.
Beide zusätzlichen bzw. vertiefenden Arbeitsschritte sind in grün gekennzeichnet.

Im Ergebnis wurden 69 verschiedene gemeinsame Einzelrisiken formuliert und angepasst.
Zusätzlich sind 19 stromspezifische Einzelrisiken definiert worden.

3.3 Prozessschritt 3, Risikoaggregation

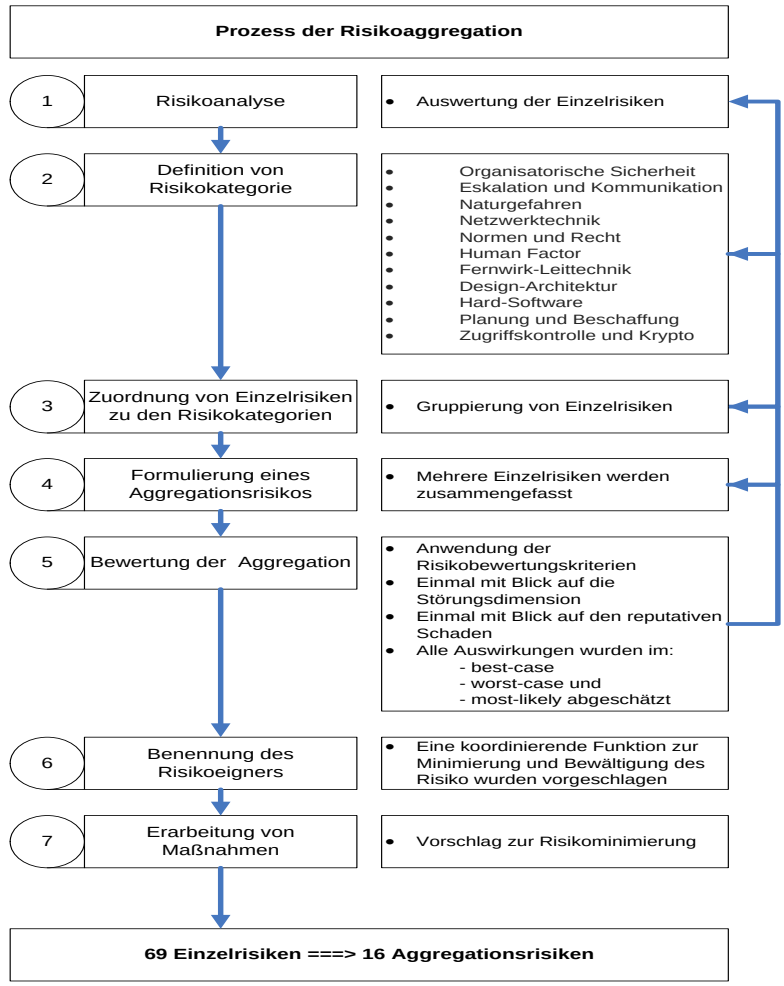


Abbildung 8: Prozess der Risikoaggregation

Der Prozessschritt der Risikoaggregation wurde methodisch analog zu den bereits durchgeführten Risikoanalysen abgearbeitet. Inhaltlich wurde die Zuordnung der veränderten Einzelrisiken zu den Aggregationsrisiken entsprechend angepasst und es wurden Doppelverwendungen von Einzelrisiken in den Aggregationsrisiken zugelassen.
Aus der Analyse und den Anpassungen bei den Einzelrisiken wurden 16 Aggregationsrisiken zusammengefasst und analysiert.

Im Ergebnis wurden 16 Aggregationsrisiken formuliert.

3.4 Prozessschritt 4, Erarbeitung von Empfehlungen

Aus der Analyse der Einzel- und Aggregationsrisiken wurden 36 Empfehlungen erarbeitet. In einem ersten Schritt wurde der Umsetzungssachstand bei den jeweiligen Prozesseignern festgehalten und farblich gekennzeichnet. Grün eingefärbte Maßnahmennummern bedeuten, dass der Prozess bereits initiiert wurde und erste Umsetzungsergebnisse vorliegen. Bei einigen Empfehlungen/Maßnahmen kann bereits „abgeschlossen und umgesetzt“ vermerkt werden. Neu hinzugekommen ist der Versuch, einen Sicherheitslevel durch die Umsetzung von Maßnahmen zu definieren. Parallel dazu wurden die Empfehlungen mit den Vorgaben des neu erschienenen BDEW-White-Papers synchronisiert. Selbstverständlich wurden die Empfehlungen auch den Aggregationsrisiken referenziert.

Kategorie	Nr.	Empfehlung geordnet nach aufsteigender Nummer	Prozesseigner	Systemrelevant(SysR)	Relevante (R.)	Priorität	Inhaltliche Ausformulierung	Ziel-Security-Level	Anmerkung	Zuordnung zu Aggregations-risiko	BDEW
Design und Architektur	EW-I	Empfehlung Nr. 1	NB/EZ/SP	X		2	IKT-PPD	3		ALLE	4.1.1
	EW-II	Empfehlung Nr. 2	NB	X	(X)	2	IKT-PPD	2			4.1
	EW-III	Empfehlung Nr. 3	NB/EZ/SP	X		2	IKT-PPD	3		9,14	3.4, 4.4
	EW-IV	Empfehlung Nr. 4	NB/EZ/SP	X		2		1		5,4,11	4.8
Eskalation und Kommunikation	EW-V	Operationalisierung des AEC initiieren und optimieren.	ARGE AEC	X	(X)	2	IKT-PPD			ALLE	4.7.4
	EW-VI	Anzahl und Art der branchenspezifischen Übungen sollen in der CSP definiert werden. Damit verbunden sind Übungstypen in der Branche zu definieren und entsprechende KPIs (für IKT-Ereignisse) festzulegen.	OE/ÖV GW/CSP	ECA/CSP		1	IKT-PPD			9	4.5,4.7.4,4.8,
	EW-VII	Branchenübergreifende Übungen einmal im Jahr bis zur staatlichen Koordinationsnotwendigkeit vorsehen (Übungen mit einem Reifegrad durch Auswertung der KPIs hinterlegen).	BKA/AEC	X	(X)	1	BM.I/BKA/AEC	4		8,9	4.5,4.7.4,4.8,
	EW-VIII	Empfehlung Nr. 8	ECA	OE/ÖV/GW-ECA		1	IKT-PPD	1		8,9,16	4.4.1, 4.4.2, 4.8.2
	EW-IX	Empfehlung Nr. 9	AEC	OE-ECA		1	IKT-PPD	4		8,9,16	4.5,4.7.4,4.8
	EW-X	Empfehlung Nr. 10	BM.I	X		2	BM.I	4		8,9,16	3.4, 4.4, 4.8.2
	EW-XI	Empfehlung Nr. 11	OE	X		2	IKT-PPD	2		8,9,16	A, A.2, 4.7.4
	EW-XII	Empfehlung Nr. 12	NB/EZ/SP	X	X	1		2		13	4.8.2

Abbildung 9: Auszug aus den Ergebnissen der Analyse von Einzel- und Aggregationsrisiken

Im Ergebnis wurden 36 Empfehlungen zusammengestellt

Im Rahmen des PPD wurde ein Vorschlag erörtert, in welcher Form die Netzbetreiber, Erzeuger und Speicherbetreiber bzw. involvierten Prozess- und Risikoeigner ihren Umsetzungsstand nach außen im Sinne eines externen Dritten transparent machen können.

Teil II Gefahren und Kommunikationsgeflechte

4. Domänenmodell.at

4.1 Domänenmodell.at-Strom

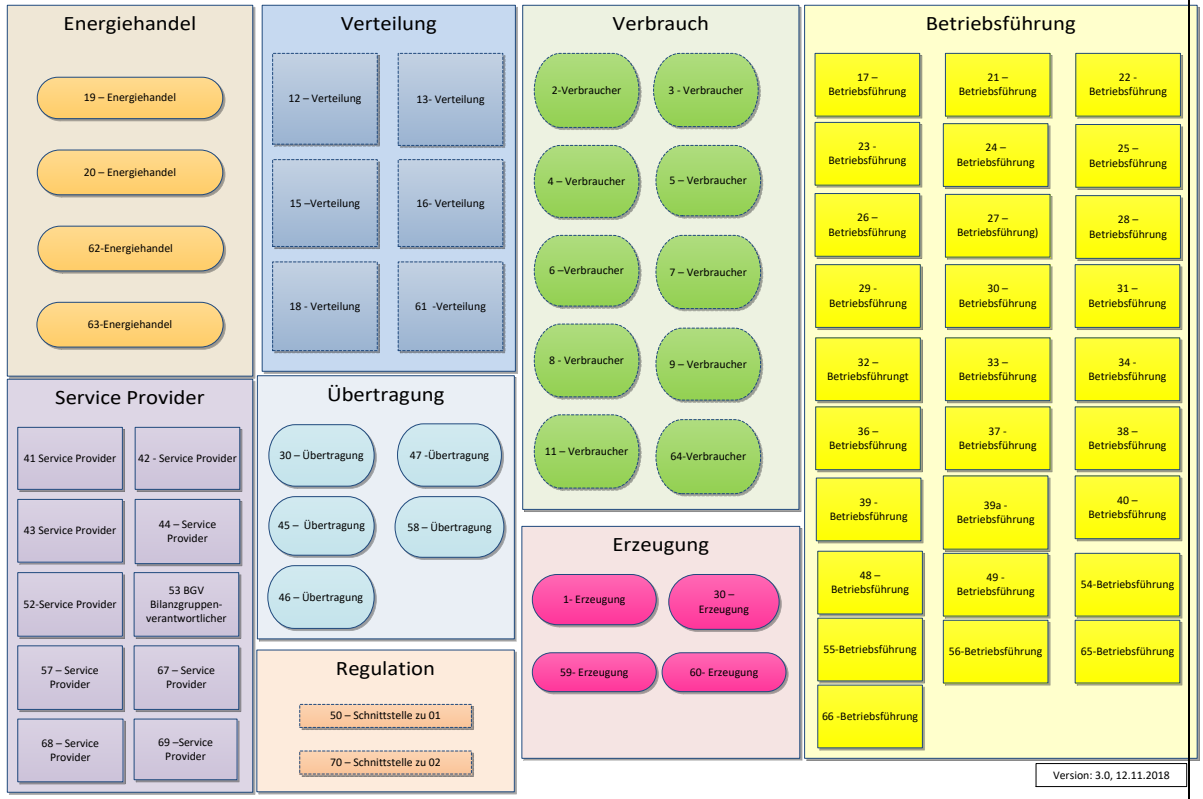


Abbildung 10: Arbeitsgruppierung kommunikativ-funktionaler Zusammenhänge

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 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. 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 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

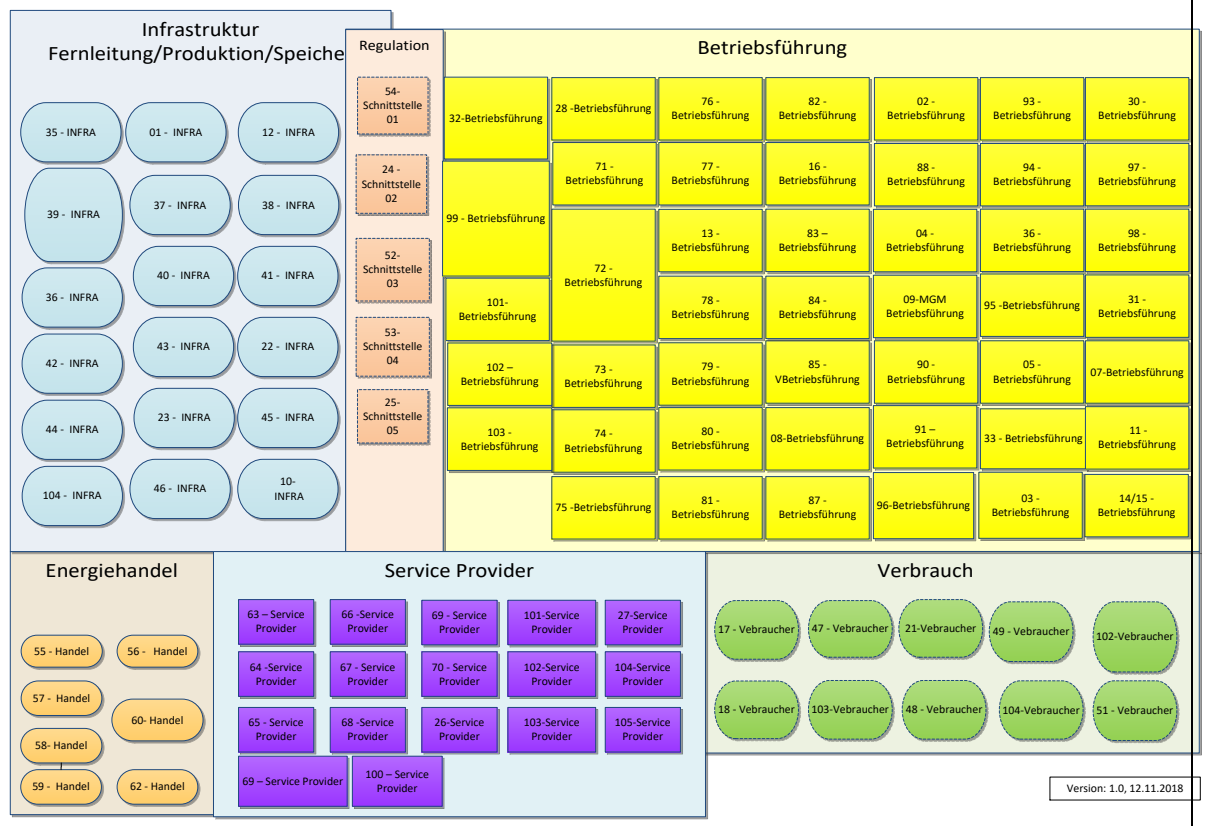


Abbildung 11: Arbeitsgruppierung kommunikativ-funktionaler Zusammenhänge

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 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. 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 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 den Kommunikationsbeziehungen wurden in Summe 226 Gefahren formuliert.
Der Gefahrenkatalog ist für Gefahrenfelder gleich aufgebaut. Er gliedert sich wie folgt:

	Gefahrenkatalog Gesamt	**Gefahrenfelder**														
Nr.	**Gefahrenbeschreibung**	**I**	**II**	**III**	**IV**	**V**	**VI**	**VII**	**VIII**	**IX**	**X**	**XI**	**XII**	**XIII**	**XIV**	**XV**
G 58	Gefahr von ….	**G**	**G**	**G**	**G**	**G**		**G**	**G**	**G**	**G**	**G**	**G**			
G 59	organisatorische Defizite …..			**G**			**G**			**G**						
S 02	Gefahr, dass …..	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. Risikobewertungskriterien; Grundlage der Risikobewertung

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“[1] 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 Dimension 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.

[1] Netzbetreiber, Erzeuger, Speicherbetreiber

5.2 Festlegung der Risikokriterien

Für die Bewertung der Eintrittswahrscheinlichkeiten von Naturereignissen und technischen Gefahren bzw. für die Abstufung der Machbarkeiten von intentionalen Angriffen auf die Steuerungsnetze sowie für die damit verbundenen Auswirkungsdimensionen wurde eine 5x5 Matrix herangezogen. Diese berücksichtigt sowohl den Verlust der Verfügbarkeit der Strom- und Gasversorgung, beschäftigt sich aber auch mit möglichen reputativen Schäden bei der Strom- und Gasversorgung.

Teil IV Empfehlungen

6. Empfehlungen

Die nachfolgenden Empfehlungen leiten sich aus mehreren Perspektiven ab und fassen die Ergebnisse der Diskussionen aus den 11 Expertenworkshops im Zeitraum Juli 2017 bis September 2018 zusammen. Die Empfehlungen stellen daher einerseits die Auswerteergebnisse 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 mit berücksichtigt,
- die für die Branche wichtigsten Entwicklungen aus einer **übergeordneten** Sicht

diskutiert und zugeordnet.
Die verschiedenen Empfehlungen haben selbstverständlich unterschiedlichste Adressaten. Die erarbeiteten Empfehlungen, die den Einzelrisiken und Aggregationsrisiken zugeordnet wurden, sind nach interner Prüfung entsprechend umzusetzen. Viele Empfehlungen sind bereits umgesetzt. Als Risiko per se persistieren viele bereits adressierte Gefahren weiter und wurden genau aus diesem Aspekt heraus auch mit in die Risikoanalyse aufgenommen.
Die Maßnahmenempfehlungen, die sich in den Aggregationen wiederfinden, adressieren sowohl inter- als auch intraorganisatorische Weiterentwicklungen der bereits vorhandenen Sicherheitsmechanismen. 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.

6.1 Relevanz der Empfehlungen & Stakeholder

In der nachfolgenden Zusammenstellung der Empfehlungen wird zwischen:

- Systemrelevanten Betreibern (Kurzbezeichnung „SysB“) und
- Relevanten Betreibern (R)

unterschieden.

Die Unternehmen und Organisationen, die den „Systemrelevanten Betreibern“ zuzuordnen sind, stellen im Wesentlichen Betreiber wesentlicher Dienste im Sinne des NIS-Gesetzes dar. Die relevanten Organisationen im Gas und bei Strom sind in einem ersten Ansatz in den Anhängen als Vorschlag zusammengestellt.

Die Identifikation orientiert sich an den Unbundling-Vorgaben der E-Control.
Behörden sind per Definition eine „Kritische Infrastruktur“ in Österreich. Die erarbeiteten Empfehlungen richten sich selbstverständlich auch an die Kritischen Infrastrukturen.
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 Expertengremium den Umsetzungsstand darstellen und ggfs. Anpassungen vorschlagen (vgl. dazu auch Kapitel 7, PPD-Prozess in der Energiewirtschaft).

6.2 Priorisierung, Zeithorizonte der Umsetzung und Ziele

6.2.1 UMSETZUNGSHORIZONTE

Die Umsetzungshorizonte und damit auch die drei Umsetzungsprioritäten wurden evaluiert und werden wie folgt definiert[2]:

- Priorität 1, kurzfristig (vorrausichtlich bis 2 Jahre[3]), spätestens bis 2021
- Priorität 2, mittelfristig (voraussichtlich 2-5 Jahre), spätestens bis 2024
- Priorität 3, langfristige Umsetzung (voraussichtlich >5 Jahre)

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.

6.2.2 ZIEL-SICHERHEITSLEVEL (SECURITY ASSURANCE LEVEL)

Im Rahmen der Erarbeitung der Maßnahmenempfehlungen wurden auch Ziele für die Festlegung von Sicherheitsstufen definiert. Wie bereits bei den Risikobewertungskriterien zur Machbarkeit von Angriffen auf die IKT, wurden im Rahmen der Maßnahmenempfehlungen Ziele festgelegt, die einen Beitrag zur Erreichung eines determinierten Sicherheitslevels vor Angriffen verschiedenster Komplexitäten und Motivationen leisten können.

Sicherheits-level	Gruppierung wer führt Angriff	Fähigkeiten	Motivation	Mittel	Ressourcen
SL1	beiläufiger oder zufälliger Versuch	Keine Angriffs-fähigkeiten	Fehler	Unbeabsichtigt	Individuell
SL2	Internetkriminalität, Hacker	Allgemein	Gering	Einfach	Gering (isolierte Einzelperson)
SL3	Hacktivist, Terrorist	ICS spezifisch	Mittel	Komplex (Angriff)	Mittel (Hackergruppierung)
SL4	Nationalstaat	ICS spezifisch	Hoch	Komplex (Kampagne)	Erweitert (multidisziplinäre Teams)
Stufen des Sicherheitsstandards (Security Assurance Levels)					

Tabelle 2: Security Assurance Level

[2] Vorbehaltlich gesetzlicher Vorgaben

[3] Ab Beginn der Umsetzung

6.3 Übersicht der Empfehlungen

Aus den 69 Einzelrisiken, 16 Aggregationsrisiken und den 19 stromspezifischen Einzelrisiken in 9 Risikokategorien wurden 36 Empfehlungen formuliert. Diese verteilen sich auf folgende Risikokategorien wie nachstehend abgebildet:

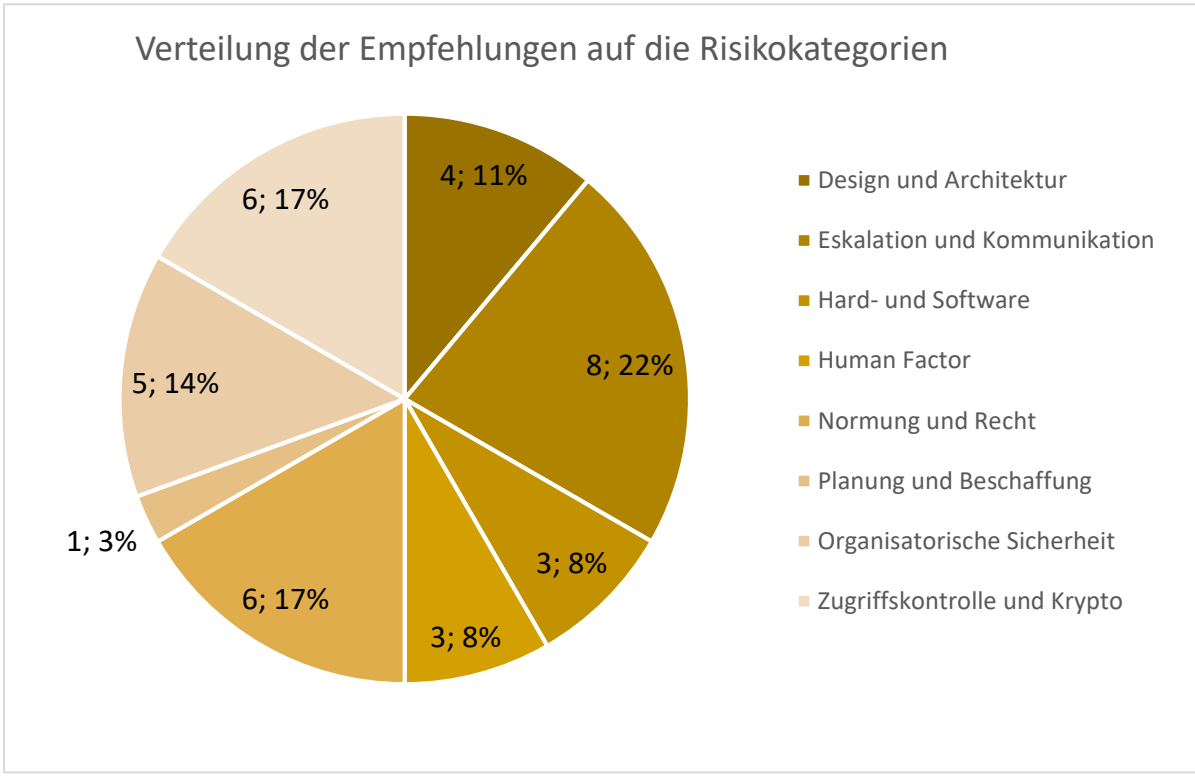


Abbildung 12: Verteilung der Empfehlungen auf die Risikokategorien

7. PPD-Prozess in der Energiewirtschaft

7.1 Allgemeines

Ein effektiver und effizienter PUBLIC-PRIVATE-DIALOG (PPD) von Risiken, die sich aus den Gefahren der Nutzung von IKT-Systemen in der Energiewirtschaft darstellen lassen, ist ein entscheidender Sicherheitsfaktor, um die Versorgungssicherheit in Österreich gewährleisten zu können. Der hier dargestellte PUBLIC-PRIVATE-DIALOG von IKT-Risiken ist daher ein wesentlicher Bestandteil des von der NIS-Richtlinie geforderten verpflichtenden IT-Risikomanagements für die Energiewirtschaft.
Der PPD basiert auf den normativen Vorgaben des „Risikomanagements" gemäß ISO 31.000 sowie der ONR 49.002-1-2. Der PPD-Prozess zur Steuerung von IKT-Risiken in der Energiewirtschaft regelt das freiwillige Zusammenwirken aller in Österreich tätigen Marktteilnehmer im Sinne der E-Control Marktregeln bei der Identifikation, Bewertung und Minimierung möglicher IKT-Risiken für bzw. in der Energiewirtschaft. Durch klar definierte Verantwortlichkeiten und einem Prozessrahmen zur Zusammenarbeit sollen Gefahren und Risiken proaktiv kommuniziert, bewältigt und minimiert werden. Der hier beschriebene Risikomanagementansatz als ***PUBLIC-PRIVATE-DIALOG-Risikomanagement Prozess (PPD-RM-Prozess)*** bereitet Grundlagen auf, um abgestimmte und wirtschaftlich vertretbare Informations- und Kommunikationstechnologie (IKT)-Sicherheitsstandards in der Energiewirtschaft umsetzen zu können.
Mit dem PPD-Prozess werden daher die Schnittstellen zwischen den gesetzlich geregelten Maßnahmen zur Umsetzung der Versorgungssicherheit, den Regelungen der NIS-Richtlinie, den Vorgaben aus dem Österreichischen Programm zum Schutz Kritischer Infrastrukturen (APCIP[4]) und abgestimmten Branchenstandards aus dem Blickwinkel von IKT-Gefahren für die Energiewirtschaft beschrieben.
Der PPD-RM-Prozess ist grundsätzlich eine freiwillige Selbstverpflichtung von Unternehmen und gilt für das Zusammenwirken zwischen der für die Energiebranche eingerichteten NIS-Behörde und Unternehmen, die „wesentliche Dienste" im Strom- und Gassektor in Österreich betreiben.

7.2 Ziele des Private Public Dialog (PPD)

Der PPD ist als Risikomanagementprozess ausgestaltet (PPD-RM). Ziel dieses Prozesses ist es, eine einheitliche Form der Risikokommunikation von möglichen IKT-Gefahren in der Energiewirtschaft aufzubauen und zu implementieren.
Mit dem PUBLIC-PRIVATE-DIAOLG wird das Zusammenwirken zwischen der NIS-Behörde, den Betreibern wesentlicher Dienste im Strom- und Gassektor, den relevanten Behörden im Sinne des APCIP den betroffenen Unternehmen und Betrieben, sowie den Interessensvertretungen des Strom- und Gassektors im Hinblick auf IKT-Risiken konkretisiert. Der PPD-Risikomanagementprozess stellt daher sicher, dass die Verantwortlichkeiten des Risikomanagementprozesses eindeutig definiert sind.

[4] APCIP, Austrian Program Critical Infrastructure Protection

Es werden somit folgende Teilziele verfolgt:

- gemeinsame und optimierte Identifikation von IKT-Gefahren und -Chancen für die Energiewirtschaft
- Schaffung einheitlicher Kriterien zur Bewertung von Gefahren zu Risiken
- Aufbau und Vertiefung von gegenseitigem Vertrauen bei allen Stakeholdern, IKT-Gefahren entsprechend professionell begegnen zu können
- Schaffung der Grundlagen eines österreichweit einheitlichen IKT-Sicherheitsniveaus für die Energiebranche
- Optimierung des Ressourceneinsatzes bei der Identifikation, Bewertung und Bewältigung von IKT-Risiken, auch unter Einbeziehung des AEC
- Abstimmung und Implementierung risikopolitischer Grundsätze innerhalb der Branche
- Klarheit über die **Aufbauorganisation** im IKT-PPD
- Klarheit über die Ablauforganisation im IKT-PPD
- Klarheit über die IKT-PPD-Prozesse im Risikomanagement
- Klarheit über die Prozesse der Risikoüberwachung und -steuerung
- Klarheit über die Eckpfeiler eines entscheidungs- und zielorientierten Berichtswesens.

Die aus dem PPD-RM-Prozess formulierten Maßnahmenempfehlungen sind grundsätzlich bindend für die am PPD-RM-Prozess teilnehmenden Unternehmen, da es sich hier um eine freiwillige Selbstverpflichtung handelt.
Die letztendliche Entscheidung über die Umsetzung der Empfehlungen und über die Höhe des akzeptierten Restrisikos, die sich daraus ergibt, verbleibt auch weiterhin bei jenen Organisationen / Unternehmen, die diese Entscheidungen auch ohne die Existenz des PPD-RM zu treffen hätten. Sie tragen daher auch die **Letztverantwortung** für die betreffenden Risiken.

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, Übersicht über die IEC-Strukturen und Implementierungen; http://smartgridstandardsmap.com
- Lit. ECA-15, Österreichisches Sicherheitshandbuch; https://www.sicherheitshandbuch.gv.at

Abkürzungsverzeichnis

Abkürzung	Erklärung
(D) DOS	Distributed Denial of Service
AEC	Austrian Energy Cert
AMI	Advanced Metering Infrastructure Headend
APCIP	Austrian Program Critical Infrastructure Protection
APCIP	Österreichisches Prorgamm zum Schutz kritischer Infrastrukturen
APT	Advanced Persistent Threat
BCM	Business Continuity Management
BKA	Bundeskanzleramt
BM.I	Bundesministerium für Inneres
CERT	Computer Emergency Response Team
CIS	Customer Information System
CSP	Cybersecurity Plattform
CSR	Customer Service Representative
DMS	Distribution Management Systems
DRMS	Demand Response Management System
ECA	E-Control Austria
EMS	Energy Management System
ENISA	Europäische Agentur für Informationssicherheit
EPCIP	European Program Critical Infrastructure Protection
EPCIP	Europäisches Programm „Schutz Kritischer Infrastrukturen“
ESP	Energy Service Provider
EUMD	Energy Usage Metering Device
EVUs	Energieversorungsunternehmen
GIS	Geographisches Informations System
HAN	Home Area Network
IDS	Intrusion Detection System
IKT	Informations- und Kommunikationstechnologie
IM	Incident Management
IoT	Internet of Things Produkte
IPS	Intrusion Prevention System
IS	Internetservices
ISMS	Informationssicherheitsmanagementsystem
ISO	Independent System Operator
ISO	International abgestimmte Norm
KI	Kritische Infrastrukturen
KPI	Key Performance Indikator
KRITIS	Kritische Infrastrukturen
KVP	kontinuierlicher Verbesserungsprozess
LMS/DRMS	Load Management Systems/Demand Response Management System

Abkürzung	Erklärung
LSA	Lenkungsausschuss
MDMS	Meter Data Management System
NB	Netzbetreiber
NIS	Netz- und Informationssicherheit in der Union
OE	Österreichs Energie
OMS	Outage Management System
ONR	Österreichische Normenregel
ÖSCS	Österreichische Strategie zur Cybersicherheit
ÖSCS	Österreichische Strategie zur Cybersicherheit
ÖVGW	Fachverband Gas-Wärme
PDCA	Plan Do Check Act
PKI	Public Key Infrastructure
PMU	Phasor Measurement Unit
PPD	Private Public Dialog
PPD-AG	Expertenarbeitsgruppe
PPD-BEI	Beirat Cybersicherheit in der Energiewirtschaft
PPD-RE	Private Public Dialog Risikoeigner
PPD-RM	Private Public Dialog Risikomanagement
PPP-Prozess	Private Public Partnership
RTO	Regional Transmission Organization Wholesale Market
RTO/ISO	Independent System Operator/Regional Transmission Organization Wholesale Market
RTU	Distribution Remote Terminal Unit
RZF	Regelzonenführer
SCADA	supervisory control and data acquisition
SKKM	Staatliche Krisen und Katastrophenmanagement
USV	Umfassende Sicherheitsvorsorge
USV	Unterbrechungsfreie Stromversorgung
WAMS	Wide Area Measurement System
WMS	Work Management System