Rundfunk & Telekom
Regulierungs-GmbH

Bericht

IKT Branchen Risikoanalyse

Version 1.0
RTR-RELEASE TO PUBLIC

Auftraggeber: RTR GmbH	Gesamtzahl Seiten: 46
Aufgabensteller: Mag. U. Latzenhofer	Anzahl Tabellen: 6
Studienkennziffer: entfällt	Anzahl Abbildungen: 15

Wien, 05.02.2018

Koordinierender Verfasser: DI Wolfgang Czerni, MBA

Kurzfassung

Die IKT-Branchenrisikoanalyse wurde in einem Private Public Partnership (PPP) Prozess im Rahmen von elf Workshops im Zeitraum März bis November 2017 erarbeitet.
Die Ergebnisse wurden in einer Expertengruppe bestehend aus Vertretern von Telekommunikations- (TELKO) und Internetserviceprovidern (ISPs) unterschiedlicher Organisationsgrößen, Interessensvertretung der Internetserviceprovider in Österreich sowie unter aktiver Beteiligung von BMVIT, BM.I, BKA und der RTR GmbH erarbeitet.
Im Rahmen der Arbeiten wurde ein 487 Gefahren umfassender Gefahrenkatalog zusammengestellt, der die wesentlichen Gefahren für die TELKO und ISP-Branche berücksichtigt und nach verschiedenen Gesichtspunkten der Informationssicherheit strukturiert ist.
Aus diesen Gefahren wiederum wurden 125 Risiken bewertet und in weiterer Folge zu 14 Aggregationsrisiken komprimiert.
Für alle Einzel- und Aggregationsrisiken wurden unmittelbar wirksame Risikominimierungsmaßnahmen konzipiert und in 12 Risikokategorien zusammengefasst:

1. Beschaffung
2. Betrieb
3. Crypto und Zugriffskontrolle
4. Design und Architektur
5. Eskalation und Kommunikation
6. Hard- und Software
7. Human Factors
8. Intentionale Gefahren
9. Naturgefahr
10. Normung und Recht
11. Organisatorische Sicherheit
12. Technik und Infrastruktur

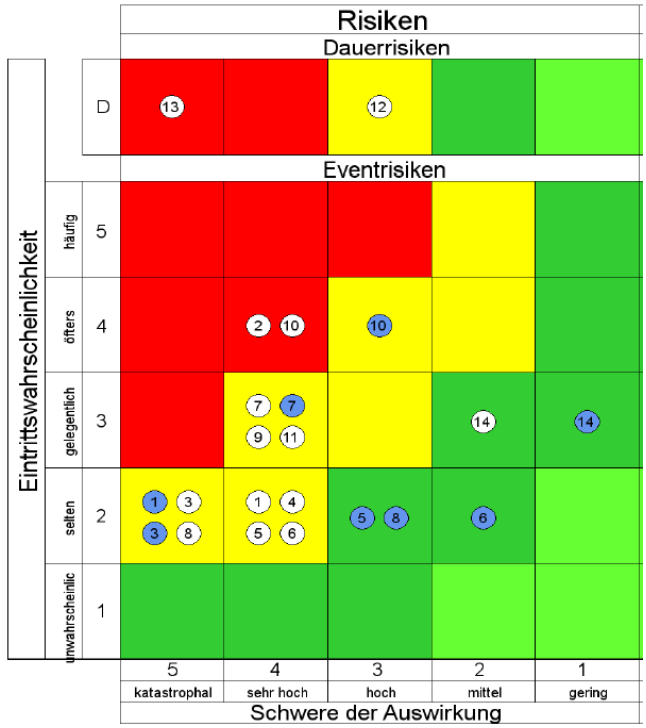
Alle identifizierten Gefahren wurden unter mehreren Gesichtspunkten zu Risiken bewertet und analysiert. Grundsätzlich wurden zwei Risikosichten gewählt: einmal die primär betriebliche Sicht der Verfügbarkeit, Aufrechterhaltung bzw. Störung der Integrität und Verlust der Vertraulichkeit und in zweiter Linie eine monetäre Bewertung von Gefahren. Hier ist klar abzugrenzen, dass die Versorgungssicherheit mit Telekommunikations- und Internetservicedienstleistungen gegenüber den rein finanziellen Risiken für die jeweilige Organisation im Vordergrund steht.

Alle Risiken wurden grundsätzlich in einem „Worst Case“, „Best Case“ und selbstverständlich in einer Erwartungssicht, dem „Most-Likely“-Fall bewertet bzw. dargestellt. Aufgrund der besonderen Eigenheit der TELKO- und ISP-Branche wurden diejenigen Schadereignisse, die ständig bzw. mit sehr hohen Frequenzen auftreten, auf einer eigenen Risikoachse dargestellt.

Um die Maßnahmenumsetzung zur Risikominimierung 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 14 Aggregationsrisiken wurde der „Worst-Case"-Fall herangezogen. Es wurden für die Betrachtung drei hohe Risiken und 9 mittlere Risiken bewertet.



- » 13, Verwundbarkeiten bei Hard- und Software
- » 02, Vorsätzliche Beschädigung, Zerstörung, Diebstahl wichtiger Betriebsmittel
- » 10, Vertraulichkeitverlust von geschützten Informationen
- » 07, Mangelhaftes Notfall-, Krisen- und Kontinuitäts-Management
- » 12, Mängel in der Betriebsführung
- » 09, Defizite bei Identity und User Access Control (IAM)
- » 11, Ausfall oder erhebliche Serviceeinschränkungen bei/von singulären IKT-Lieferanten
- » 03, Kriminelle Handlungen aus dem Cyberraum
- » 08, Erhebliche Probleme beim Patch- und Updateprozess
- » 01, Ausfall wesentlicher Infrastrukturen
- » 04, Mögliche erhebliche Defizite bei IKT-Designfragen
- » 05, Negative Auswirkungen von politisch-rechtlichen Rahmenbedingungen
- » 06, Defizite im Beschaffungsprozess

Die Risiken in blauer Farbe wurden in monetärer Hinsicht bewertet. Risiko Nr. 13 beschäftigt sich mit möglichen Verwundbarkeiten durch APTs (Advanced Persistent Threats), die im Worst Case „katastrophale" Auswirkungen auf den Sicherheitslevel haben können. Risiko Nr. 2 fasst de facto drei wesentliche Aspekte betrieblicher Verfügbarkeitsaspekte zusammen. Einmal ungewollte, aber leider sehr häufig vorkommende Manipulationen im Boden und damit verbunden Unterbrechungen bei wichtigen Verteilnetzen. Ein zweiter aggregierter Aspekt bezieht sich auf den Diebstahl von Equipment, der sich u. a. auch auf vital wichtige Systeme beziehen kann. Ein dritter Aspekt beschäftigt sich mit der physischen Sicherheit von IKT-Equipment. Risiko 10 adressiert die zunehmende Komplexität, kryptographische Methoden effektiv zu implementieren und deren Wirksamkeit über den gesamten Life-Cycle hinweg auch „nachzuweisen".
Zu jedem Einzel- und Aggregationsrisiko wurden Minimierungsmaßnahmen vorgeschlagen. Viele davon sind in den meisten Unternehmen bereits umgesetzt.

Daraus ergeben sich insgesamt 37 Empfehlungen, die für die Optimierung der Informationssicherheit - aus drei wesentlichen Blickwinkeln betrachtet – wie folgt zusammengefasst werden können:

- Vorschläge und Empfehlungen, die sich an die Organisationen selbst richten,
- Anregungen, die einen „Stand der Technik" bei der Implementierung von Informationssicherheit definieren helfen sollen und
- Vorschläge für künftige nationale und internationale normativ-rechtliche Rahmenbedingungen, die für die Branche marktneutrale Rahmenbedingungen schaffen und Informationssicherheit effektiv umzusetzen sollen.

Empfehlungen, die sich an die Organisationen selbst richten, können wie folgt zusammengefasst werden:

- Sicherstellung der organisationsübergreifenden Funktionsfähigkeit des Business Continuity- und Krisen-Managements, u. a. durch regelmäßige Durchführung und Teilnahme an Übungen.
- Gleichrangigkeit von Securityanforderungen mit allen anderen betrieblichen Anforderungen in allen Phasen des Life-Cycles, beginnend mit der Beschaffung und Produktgestaltung bis hin zur Dekommissionierung.
- Anreicherung des betriebsinternen Risikomanagements um die Punkte des vorliegenden Gefahrenkatalogs und unter Berücksichtigung der vorgeschlagenen Maßnahmen.

Anregungen, die einen Stand der Technik und Praxis bei der Umsetzung von Informationssicherheit definieren helfen sollen, werden wie folgt zusammengefasst:

- Entwicklung von Branchenmindeststandards für „sicher konfigurierte" CPEs (beide, die von Netzbetreiber zur Verfügung gestellte und reine Kundenendgeräte), sollen in Abstimmung mit dem Regulator entwickelt werden.
- Im gesamten Life-Cycle von netzwerkfähigen Geräten (z. B. IoT) muss die Erfüllung von Informationssicherheitsanforderungen gewährleistet werden. Die Branche fordert entsprechende Entwicklungen unter Einbeziehung von Wissenschaft und Forschung und trägt zur Schaffung von EU-weiten Regelungen bei.
- Das Hinwirken auf strikte Trennung von funktionalen und securityrelevanten Patches sowie die Ausarbeitung entsprechender Testregime und Testmöglichkeiten auf europäischer Ebene wird empfohlen.
- Intensivierung des organisationsübergreifenden Informations- und Erfahrungsaustausches zu konkreten Sicherheitsimplementierungen unter Einbindung von CERT.AT.

Vorschläge für künftige nationale und EU-weite Regularien wurden zusammenfassend wie folgt formuliert:

- Die Herausforderungen durch die Vorgaben der Netzneutralität in Zusammenhang mit dem Anstieg unsicherer IoT/CPE/Mobile Devices bedürfen weiterer Sicherheitsmaßnahmen (z. B. regulative Vorgaben, entsprechende Monitoring Möglichkeiten, präventive und reaktive Handlungsoptionen seitens der Betreiber etc.)
- Die Abstimmung und die Harmonisierung von Mindestsicherheitsstandards für IKT-Produkte und Dienstleistungen auf EU-Ebene werden von den Branchenvertretern als marktneutrale und ökonomisch sinnvolle Maßnahmen zur Erhöhung der Cybersicherheit erachtet.

- Eine frühzeitige Einbindung der Branchenvertreter in den legistischen Entwicklungsprozess in einem branchenspezifischen PPP-nach Vorbild des Rechts- und Technologiedialogs wird empfohlen.
- Aus Sicht der Branche stellen absichtliche Backdoors und Schwächungen von Sicherheitsmechanismen ein schweres Sicherheitsrisiko dar und werden daher klar abgelehnt.
- Der Abgleich des hier vorliegenden Branchenrisikokatalogs mit jenen von anderen Sektoren der kritischen Infrastrukturen ist notwendig, um sektorübergreifende und sektorspezifische Sicherheitsmaßnahmen erkennen und adressieren zu können.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Teil I Methodik und Vorgehensweise

1. Grundsätzlicher Aufbau der Risikoanalyse

Die Risikoanalyse liegt in vier Teilen vor. Teil I beschreibt die allgemeine Herangehensweise und Methode zur Risikoidentifikation und Bewertung. Die Vorgehensweise orientiert sich an den Vorgaben der „ISO 31.000:2010 risk management", „ISO 31.010:2010 risk assessment techniques" und der ONR 49.002-2:2010, Risikomanagement für Organisationen und Systeme, Leitfaden für die Methoden der Risikobeurteilung.
Im ersten Teil wird auch eine „Wissensbasis" beschrieben, die eine spezifische Literaturzusammenstellung aufbereitet.
Der Teil II, Kontexterfassung, befasst sich mit der Einbettung der Branchenrisikoanalyse in nationale Programme und Vorgaben zur Cybersicherheit sowie mit der aktuellen Schnittstelle zur Umsetzung der NIS[1]-Richtlinie in ein „Bundesgesetz für Cybersicherheit[2]"
Im Teil III, Ergebnisdarstellung, wird der während der verschiedenen Workshops erarbeitete Gefahrenkatalog dargestellt und die darauf aufbauenden Einzelrisiken. In einem weiteren Schritt werden die Aggregationsrisiken zusammengefasst und diskutiert. Der Teil III stellt somit die Ergebnisse der Gefahrenidentifikation und Bewertung zu Risiken dar.
Aus der Zusammenschau aller Einzel- und Aggregationsrisiken wurden Maßnahmen & Empfehlungen abgeleitet, die im Teil IV zusammengestellt werden.

2. Zielsetzungen und Hintergrund der Risikoanalyse

2.1 Allgemeines

Der vorliegende Bericht soll die Grundlagen für eine Branchenrisikoevaluation schaffen. Im Rahmen der weiteren Arbeitsschritte werden unter *„Telekommunikationsbranche"* folgende Unternehmen zusammengefasst:
(a) Alle Unternehmen, die die Bereitstellung eines öffentlichen Kommunikationsnetzes oder -dienstes gemäß § 15 TKG 2003 angezeigt haben oder verpflichtet gewesen wären, diesen anzuzeigen und diesen nicht eingestellt haben.
(b) Alle in Österreich niedergelassenen Betreiber wesentlicher Dienste iSd Art 4 Z 4 RL (EU) 2016/1148, die dem Sektor "digitale Infrastruktur" iSd Anh II Z 7 RL (EU) 2016/1148 zuzurechnen sind.

2.2 Zielsetzungen der Risikoanalyse

Das Ziel der vorliegenden Risikoanalyse ist es, Gefahren zu identifizieren, die eine **nennenswerte** Auswirkung auf die durch Telekomunikations- und Internetserviceprovidern erbrachten Dienstleistungen durch:

- die Nutzung und Anwendung von Informations- und Kommunikationstechnologie(n)

[1] Siehe Lit.RTR-24, RICHTLINIE DES EUROPÄISCHEN PARLAMENTS UND DES RATES über Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit in der Union, kurz NIS-Richtlinie

[2] Derzeitiger Arbeitstitel des Gesetzes

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

haben können. Insbesondere bei „Intentionalen Gefahren" werden Belange des Datenschutzes mit angesprochen.

Eine bindende Festlegung bzw. eine Definition für „Vorfälle mit beträchtlichen Auswirkungen auf die Verfügbarkeit von Kommunikationsnetzen oder –dienste" ist in § 16a Abs. 5 TKG 2003 geregelt. Hier haben Betreiber öffentlicher Kommunikationsnetze oder -dienste der Regulierungsbehörde Sicherheitsverletzungen oder einen Verlust der Integrität in der von der Regulierungsbehörde vorgeschriebenen Form mitzuteilen, sofern dadurch beträchtliche Auswirkungen auf den Netzbetrieb oder die Dienste-Bereitstellung eingetreten sind.

Für eine allgemeine Risikobetrachtung, die alle Aspekte der Ziele der Branchenrisikoanalyse abdecken soll, wurde eine geeignete Abstufung der Signifikanz von Auswirkungen auf die Telekommunikations- und Internetserviceprovider (in weiterer Folge nur mehr TELKOs bzw. ISPs genannt) im Rahmen der Workshops erarbeitet.

2.3 Nichtziele der Risikoanalyse

Obwohl sich die identifizierten Risiken auch mit monetären Auswirkungen der verschiedenen Gefahren beschäftigen, stehen **nennenswerte** Auswirkungen auf die

- Verfügbarkeit,
- Integrität,
- und Vertraulichkeit

der angebotenen Serviceleitungen der TELKOs und ISPs im Vordergrund. Die Erhebung bzw. Identifikation von ausschließlich monetären Aspekten, also primär rein privatwirtschaftliche Risiken, sind nicht Gegenstand der Erhebungen, obwohl sie zum Teil indirekt mitbetrachtet wurden. Diese Betrachtungen dienen dann eher der gesellschaftlichen Abschätzung der Bedeutung von aufgezeigten Schadwirkungen.

2.4 Allgemeine Rahmenbedingungen der Risikoanalyse

Im Rahmen der Risikobewertungen müssen Aussagen zu „Erwartungswerten" für Stör- oder Schadereignisse prognostiziert oder besser abgeschätzt werden. Der Prognosehorizont für die Erfassung und Bewertung der Risiken wurde bis 2020 festgelegt.
In vielen Fällen, insbesondere bei der Bewertung von intentionalen Gefahren, verfügt man bis dato über wenig Erfahrung bzw. belastbare Daten, um eine objektivierte „Prognose" zu Eintrittswahrscheinlichkeiten abgeben zu können. Hier wird der Begriff der Machbarkeit eingeführt.

Um für alle drei Hauptgefahrenfelder:[3]

- technische Gefahren,
- Naturgefahren und
- intentionale Gefahren,

eine einheitliche Risikomatrix abbilden zu können, wurden die Bewertungskriterien für die Eintrittswahrscheinlichkeiten für technische Gefahren und Naturgefahren zusammengefasst. Parallel dazu wurde die Eintrittswahrscheinlichkeit für intentionale Gefahren nur implizit über abgeschätzte Häufigkeiten pro Zeiteinheit von möglichen „Ereignissen, Attacken und Penetrationen" definiert, sondern vielmehr über den Begriff der Machbarkeit hergeleitet und diese in Relation zueinander gesetzt.
Es wird daher darauf hingewiesen, dass die identifizierten und bewerteten Risiken immer nur **in Relation zueinander** eine valide Aussage erlauben, da nicht der Anspruch erhoben wird, dass die identifizierten Risiken eine *absolute* Position in der Risikomatrix einnehmen.

3. Methodik der Risikoanalyse

Die Risikoanalyse wurde gemäß den Rahmenvorgaben der ISO 31.000 bzw. der ONR 49.002-1-2:2010 durchgeführt. Dazu wurden seitens der Rundfunk und Telekomunikations Regulationsbehörden (RTR) 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
- Ein erweitertes Projektteam von Experten bei TELKOs und ISPs sowie deren Interessensvertretung (ISPA)

[3] Siehe ÖNORM S2401, Business Continuity und Corporate Security Management, "Systemaufbau und Business Continuity und Corporate Security Policy"

3.1 Übersicht des Risikoidentifikations & Bewertungsprozesses

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

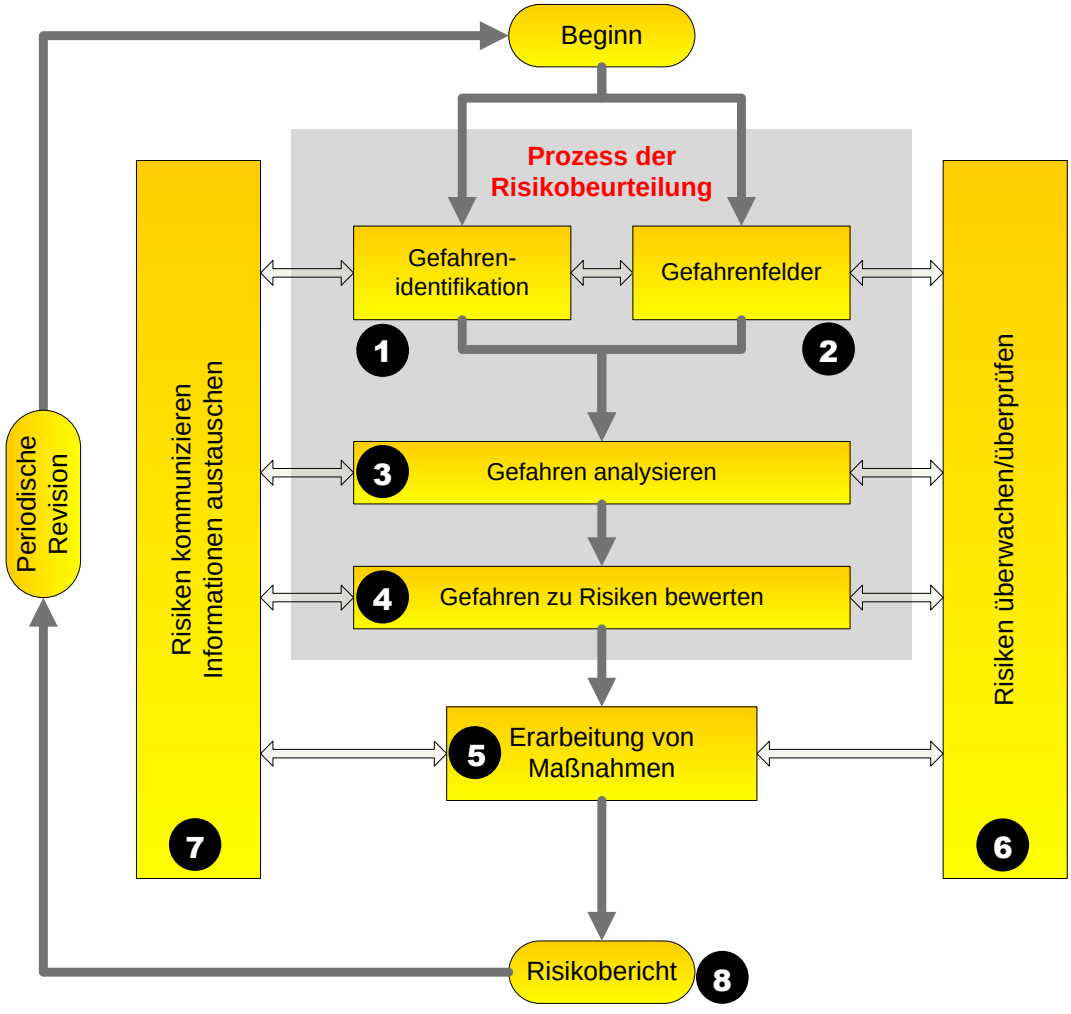


Abbildung 1: Vorgehensweise in der Risikoanalyse

3.1.1 PROZESSSCHRITT 1, GEFAHRENIDENTIFIKATION

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

- Verfügbarkeit
- Vertraulichkeit und
- Integrität

gestört werden kann bzw. wird. Als wesentlichster Schritt wird die Erarbeitung eines umfassenden Gefahrenkatalogs erachtet, wobei bestehende Gefahrenkataloge als Grundlage für die Zusammenstellung des Gefahrenkatalogs herangezogen wurden. Es sind dies u. a.:

- ENISA Guideline for threats and assets - V1.1, March 2015 (ENISA-GL)

- ITU-T - SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY Telecommunication security (ITU-T-REC-X)
- ISO/IEC 27001 - Information security management systems – Requirements (ISO-27001)
- ISO/IEC 27002 - Information technology — Security techniques Code of practice for information security controls (ISO-27002)
- 7 Layers of OSI (OSI-7-L)
- BSI IT-Grundschutzkataloge (BSI-IT-GS)

3.1.2 PROZESSSCHRITT 2, GEFAHRENFELDER

Die im Prozessschritt 1 erarbeiteten Gefahren wurden in 11 Gefahrenfelder eingeteilt. Diese 11 Bereiche wurden für die systematische Identifikation von Risiken herangezogen.

3.1.3 PROZESSSCHRITT 3, GEFAHRENANALYSE

In den jeweiligen Gefahrenfeldern wurden während der Workshops auf Basis eigener Erfahrungen zusätzliche Gefahren in die Gefahrenfelder eingearbeitet und analysiert. In Summe wurden 487 Einzelgefahren zusammengestellt und in weiterer Folge analysiert.

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 7)
- Phase II, Bewertung der 487 identifizierten Gefahren zu 125 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 125 Einzelrisiken zu 14 Aggregationsrisiken

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 15.11.2017 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.

4. Aufbereitung der Literatur & Recherchen

Um fortfolgende Arbeiten optimal zu unterstützen, wurden alle Zwischenergebnisse und Ergebnisse in den Anhängen zusammengestellt und aufbereitet. Die Datengrundlagen und erarbeiteten Risikomatrizen liegen auf einer CD-R so aufbereitet bei, dass diese bei Bedarf in ein Intranet übernommen werden bzw. auf elektronischem Weg ausgetauscht werden können. Der Bericht verweist auf die in der Quellensammlung zusammengestellten Literaturstellen wie folgt:

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

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

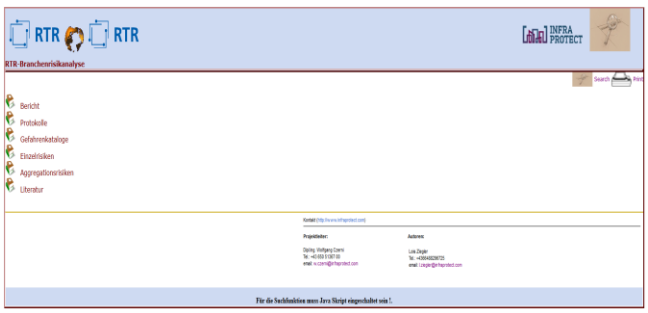


Abbildung 2: Literaturzusammenstellung

Bei Anfragen von Kunden ermöglicht dies den direkten Zugriff auf nicht als Datei zur Verfügung gestellte klassifizierte oder urheberrechtlich geschützte Literatur.

Das entsprechende wissenschaftliche Zitat kann über die Suchfunktion auf der beiliegenden CD-R direkt gesucht werden.

Es kann auch nach Schlagworten recherchiert werden (interne, offline „Google Suche“, ausführbar auch ohne Zugriff aufs Internet. Bitte beachten Sie, dass durch Sicherheitseinstellungen Ihres Browsers die Suchfunktion eingeschränkt sein könnte).
Urheberrechtlich geschützte Werke, insbesondere Normen, werden lediglich zitiert. Frei verfügbare Literatur, wie z. B. alle ENISA Dokumente oder die BSI-Kataloge werden als Dateien der Literaturzusammenstellung beigelegt.

Teil II Kontexterfassung

5. Die Österreichische Sicherheitsstrategie

Österreich verwirklicht seine Sicherheitspolitik im Rahmen des Konzepts der „Umfassenden Sicherheitsvorsorge“ (USV). Diese zielt auf das systematische Zusammenwirken verschiedener Politikbereiche auf Basis einer Gesamtstrategie und der relevanten Teilstrategien ab. Ein umfassendes Lagebild aller Akteure und ein darauf aufbauendes gemeinsames Lageverständnis sind notwendige Grundlagen für sicherheitspolitische

Entscheidungen auf nationaler und internationaler Ebene. Dabei sollen Synergien im Sicherheitsbereich im Rahmen eines gesamtstaatlichen „Sicherheitsclusters“ erzielt werden.
Die im Juli 2013 beschlossene „Österreichische Sicherheitsstrategie“ betrachtet das Thema Sicherheit aus den Blickwinkeln der inneren Sicherheit, der Außenpolitik und der Verteidigungspolitik. Das Thema Cybersecurity wird in dieser Strategie explizit mehrmals angesprochen. Abgeleitet von der USV werden in Österreich daher parallel mehrere Teilstrategien, Sicherheits- und Schutzkonzepte entwickelt.

5.1 APCIP, Österreichisches Programm zum Schutz Kritischer Infrastrukturen

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

5.2 IKT-Sicherheitsstrategie

Im Frühjahr 2012 wurde durch das Bundeskanzleramt (BKA) gemeinsam mit Expertinnen und Experten aus Wirtschaft, Wissenschaft und öffentlicher Verwaltung eine IKT Sicherheitsstrategie entwickelt. Diese Strategie hat als Kernziele die kritischen Informationsinfrastrukturen und deren Schutz und fordert davon ausgehend die Umsetzung von Maßnahmen zur Festigung und Handlungsschemata, die die Kalkulierbarkeit der Risiken sicherstellen (Risikomanagement und Lagebild). Weitere Schwerpunkte sind die Themen Bildung und Forschung sowie das Thema Awareness.
Im Kontext zur vorliegenden Risikoanalyse sind vor allem die Vorgaben für den Schutz Kritischer Infrastrukturen relevant.
Es wird die Förderung des Risikomanagements innerhalb der Kritischen Infrastruktur explizit gefordert. Der Staat soll die Unternehmen dabei durch Maßnahmen wie Abgleich von Informationen zur gemeinsamen Risikoanalyse, Akkreditierung von Risikomanagement-methoden, Angleichung von Ausbildungsmaßnahmen, Analysen der Technologiefolgenabschätzung und den Einsatz von Sanktionen und Anreizen unterstützen.
Weiter werden in diesem Bereich die Einrichtung eines Cyber-Krisenmanagements, der Aufbau eines Cyber-Lagezentrums und das Einrichten einer tragfähigen Krisenkommunikation gefordert. Das Cyber-Lagezentrum soll einen Überblick über die aktuelle Cyber-Situation ermöglichen und würde die bereits durch andere Einrichtungen (z. B. CERTs) wahrgenommenen Aktivitäten an einer zentralen Stelle bündeln. Bezüglich der Krisenkommunikation beschreibt die Strategie, dass sie gemeinsam durch gesicherte private und öffentliche Kommunikationsanlagen aufrechterhalten werden soll.
Das Thema Risikomanagement wird in diesem Bereich nochmals betrachtet, allerdings vor allem aus dem Blickwinkel der Forderung nach sektorübergreifenden Maßnahmen sowie der Sicherstellung von Mindeststandards. Die Motivation dafür entsteht aus der Einschätzung, dass jeder Sektor für sich ein gut ausgeprägtes Risikomanagement hat, eine übergreifende Risikobetrachtung aber fehlt.
In Bezug auf die Etablierung von Mindeststandards erwartet die Strategie eine Diskussion dazu, in welcher Form Mindeststandards verankert werden können (als Gesetze, Richtlinien, Normen, etc.) und zur Kontrolle der Einhaltung. Durch Umsetzung dieser Mindeststandards

soll vor allem vermieden werden, dass aufgrund betriebswirtschaftlicher Überlegungen auf eine Risikovorsorge verzichtet wird.

5.3 Zusammenführung in die ÖSCS

Die Ergebnisse der IKT-Sicherheitsstrategie und der Cybersecurity Initiative des BM.I wurden in einer Kooperation des Bundeskanzleramtes, des Verteidigungsministeriums und des Innenministeriums zur Erstellung einer nationalen Cybersecurity Strategie genutzt – der „Österreichischen Strategie für Cybersicherheit (ÖSCS)".
Diese Strategie definiert unter anderem die Einrichtung einer Steuerungsgruppe und deren Zusammenarbeit mit privaten Akteuren aus Wirtschaft und Forschung, die Schaffung einer Struktur zur Koordination auf operativer Ebene und das bereits in der IKT Sicherheitsstrategie geforderte Cyber Krisenmanagement. Diese Strategie wurde im März 2013 beschlossen und aktuell sind mehrere interministerielle Arbeitsgruppen mit der Umsetzung befasst.
Die ÖSCS hat vor allem die Forderungen der IKT-Sicherheitstrategie nach einer Erstellung eines periodischen und anlassbezogenen „Lagebild Cyber Sicherheit" und nach der Einbindung der Betreiber kritischer Infrastrukturen in die Prozesse des nationalen Cyber Krisenmanagements übernommen.
Auf rechtlicher Basis soll ein Bericht zu einem zeitgemäßen ordnungspolitischen Rahmen erstellt werden, der rechtliche Grundlagen und regulatorische Maßnahmen sowie nicht-rechtliche Selbstverpflichtungen prüft. Über eine gemeinsame Arbeit aller relevanten Stakeholder sollen Mindestsicherheitsstandards für Cybersicherheit definiert werden.
Zur Umsetzung der ÖSCS wurde eine interministerielle Steuerungsgruppe eingerichtet, die wiederum 4 interministeriellen Arbeitsgruppen, aus den ÖSCS abgeleiteten Teilaufgaben zugeordnet hat:

- Operative Koordinierung (Erstellung eines Lagebildes, Beratung über zu treffende Maßnahmen auf operativer Ebene, Schaffung einer Struktur, die als operatives Ausführungsorgan für ein übergreifendes Cyber Krisenmanagement genutzt werden kann)
- Erstellung eines Berichtes zum ordnungspolitischen Rahmen (rechtliche Grundlagen, regulatorische Maßnahmen, nicht-rechtliche Selbstverpflichtungen, Anreize und Sanktionen)
- Einrichtung einer Cyber Sicherheitsplattform (ständiger Informationsaustausch der öffentlichen Verwaltungen untereinander sowie der öffentlichen Verwaltung mit Vertretern der Wirtschaft, Wissenschaft und Forschung)
- Erstellung einer Kommunikationsstrategie (Abstimmung der bereits eingerichteten und geplanten staatlichen Websites)

Diese Arbeitsgruppen haben im Sommer 2013 ihre Arbeit aufgenommen.

5.3.1 ÜBERSICHT ÜBER DIE DERZEITIGE CYBERSECURITY -LANDSCAPE

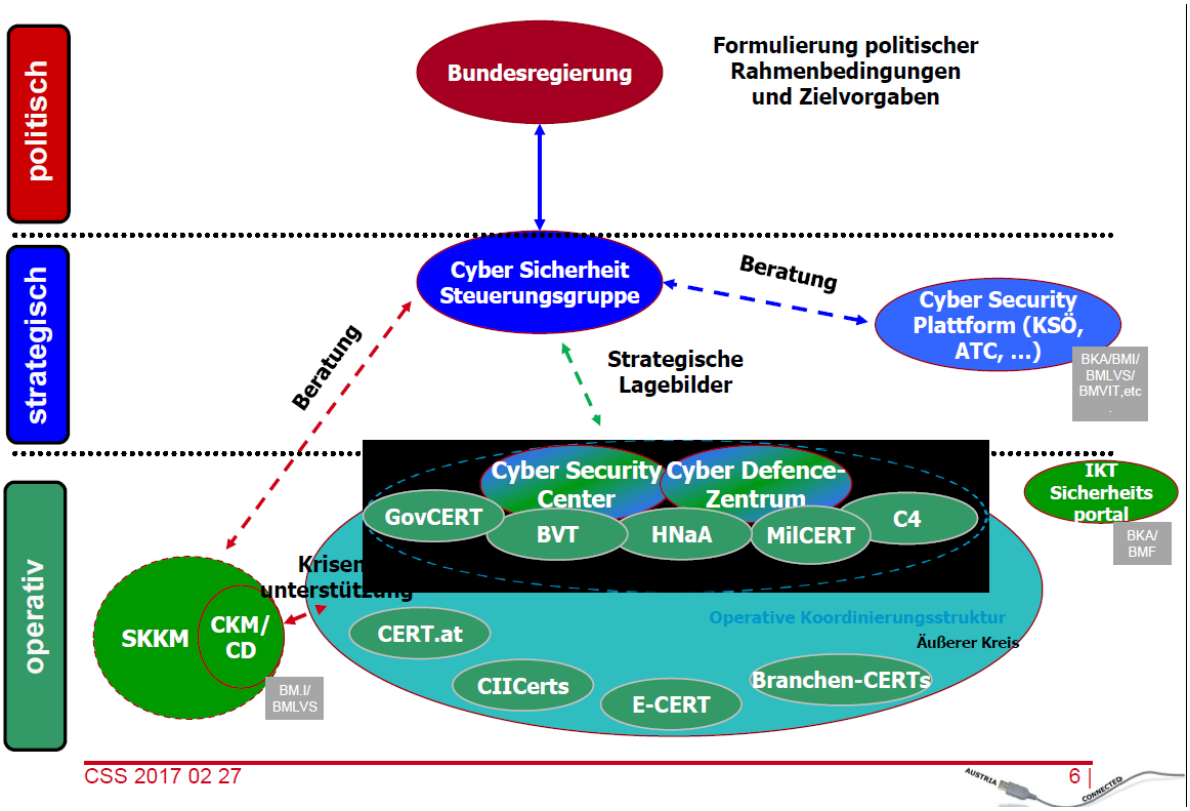


Abbildung 3: Cybersecurity Kontext in Österreich

5.4 Umsetzung der NIS-Richtlinie Ausblick

Mit dem 2013 veröffentlichten Vorschlag für eine „RICHTLINIE DES EUROPÄISCHEN PARLAMENTS UND DES RATES 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 erfolgt mittels des Bundesgesetzes für Cybersicherheit. Unter die NIS-Richtlinie fallen Betreiber wesentlicher Dienste, wobei die den Betreibern wesentlicher Dienste und den Anbietern digitaler Dienste auferlegten Verpflichtungen nicht für Unternehmen gelten, die öffentliche Kommunikationsnetze oder öffentlich zugängliche elektronische Kommunikationsdienste im Sinne der Richtlinie 2002/21/EG des Europäischen Parlaments und des Rates (1) bereitstellen und die den besonderen Sicherheits- und Integritätsanforderungen jener Richtlinie unterliegen. Das bedeutet, dass diese Betreiber nur in jenen Bereichen als Betreiber wesentlicher Dienste angesehen werden können, in denen sie nicht elektronische Kommunikationsdienste anbieten. Eine Liste von KRITIS-Betreibern in Österreich ist vorhanden (entsprechend nachvollziehbare Kriterien in der NIS). Abweichungen von der APCIP-Liste sind möglich. Digitale Dienste sind europaweit harmonisiert, hier gibt es keinen Spielraum für NIS. Verfassungsmäßige Einrichtungen werden freiwillig partizipieren.
Nach derzeitigem Wissensstand ist es geplant, Auditierungen von Sicherheitsstandards durch die NIS Behörden oder durch beauftragte Dienstleister vorzunehmen. In diesem Kontext spielt die Risikoanalyse eine wesentliche Rolle, da die auditierten Unternehmen

durch Festlegung von Maßnahmen de facto Branchensicherheitsstandards definieren. Zum Zeitpunkt der Übermittlung des Bescheids durch die Behörde sollte ein Unternehmen, das Betreiber wesentlicher Dienste ist, für diese Dienste bereits ISMS zertifiziert sein (pers. Info. Czerni). In Österreich soll nach derzeitigem Wissensstand die Erstüberprüfung innerhalb eines Jahres durchgeführt werden (entspricht einer Schonfrist). Ziel dabei ist es, die erste Runde im November 2018 abzuschließen.
Die Verordnungsermächtigung der NIS-Behörden legt Grenzwerte der Meldepflicht und Sicherheitsstandards fest. Die Umsetzung wird bis zum 9. Mai 2018 avisiert. Im November 2018 soll die Notifizierung an Brüssel erfolgen.
Die Betreiber kritischer Dienste im Sinne der NIS-Richtlinie werden durch einen Bescheid, der auf dem Bundesgesetz zur Cybersicherheit bzw. auf den damit verbundenen Verordnungen basiert, identifiziert. Der Bescheid beinhaltet, welche Tätigkeitsbereiche des betroffenen Unternehmens darunter fallen und welche NIS Stelle zuständig ist.
Die Verordnungstexte sollen in einer „Begutachtung" schon vorher veröffentlicht werden. Die Verordnung tritt relativ zeitnah nach Inkrafttreten des Gesetzes in Kraft.
Auf europäischer Ebene sollen Regelungen in einer Koordinationsgruppe harmonisiert werden.
Die Verordnung(en) zum Bundesgesetz wird (werden) vom Bundeskanzleramt (federführend), dem Bundesministerium für Landesverteidigung und Sport und dem Bundesministerium für Inneres erarbeitet.
Unternehmen, die öffentliche Kommunikationsnetze oder öffentlich zugängliche elektronische Kommunikationsdienste im Sinne der Richtlinie 2002/21/EG des Europäischen Parlaments und des Rates (1) bereitstellen und die den besonderen Sicherheits- und Integritätsanforderungen jener Richtlinie unterliegen, unterliegen diesbezüglich weiterhin den Regelungen des Telekommunikationsgesetzes.

Bis dato geht die RTR davon aus, dass das Melderegime gemäß § 16a Abs 5 TKG 2003 und Meldungen gemäß NIS-Richtlinie entweder harmonisiert oder klar abgegrenzt werden.

Teil III Ergebnisdarstellung

6. Gefahrenkatalog; Grundlage der Risikoidentifikation

6.1 Prozess der Gefahrenidentifikation

Die Branchenrisikoanalyse setzt sich das Ziel, möglichst umfassend alle Gefahren, die sich für TELKOs und ISPs ergeben, zu identifizieren. Dazu wurden in einem ersten Schritt die bestehenden Gefahrenkataloge ausgewertet und zusammengestellt. Da sich die Risikoanalyse jedoch primär mit branchentypischen Gefahren auseinander setzen soll, wurden determinierte interorganisatorische Gefahren einer für die Risikoidentifizierung im Vergleich weitaus geringeren Priorität zugeordnet. Die Gefahrenlandschaft wurde daher in drei Workshops auf Basis der bestehenden Gefahrenkataloge vorstrukturiert, anhand von Prioritäten vorselektiert und auf Basis der einschlägigen Erfahrungen der Experten in den Workshops ergänzt.
Im Ergebnis wurde die Gliederung des Gefahrenkatalogs in 11 Gefahrenfelder vorgenommen, die sich u. a. auch an der „Control-Struktur" der ISO 27.002 orientiert, um mit bereits bestehenden Managementsystemen ein gewisses Maß an Kompatibilität der Betrachtungen erhalten zu können. Die Struktur der Gefahrenlandschaft ist in Abbildung 4 dargestellt.

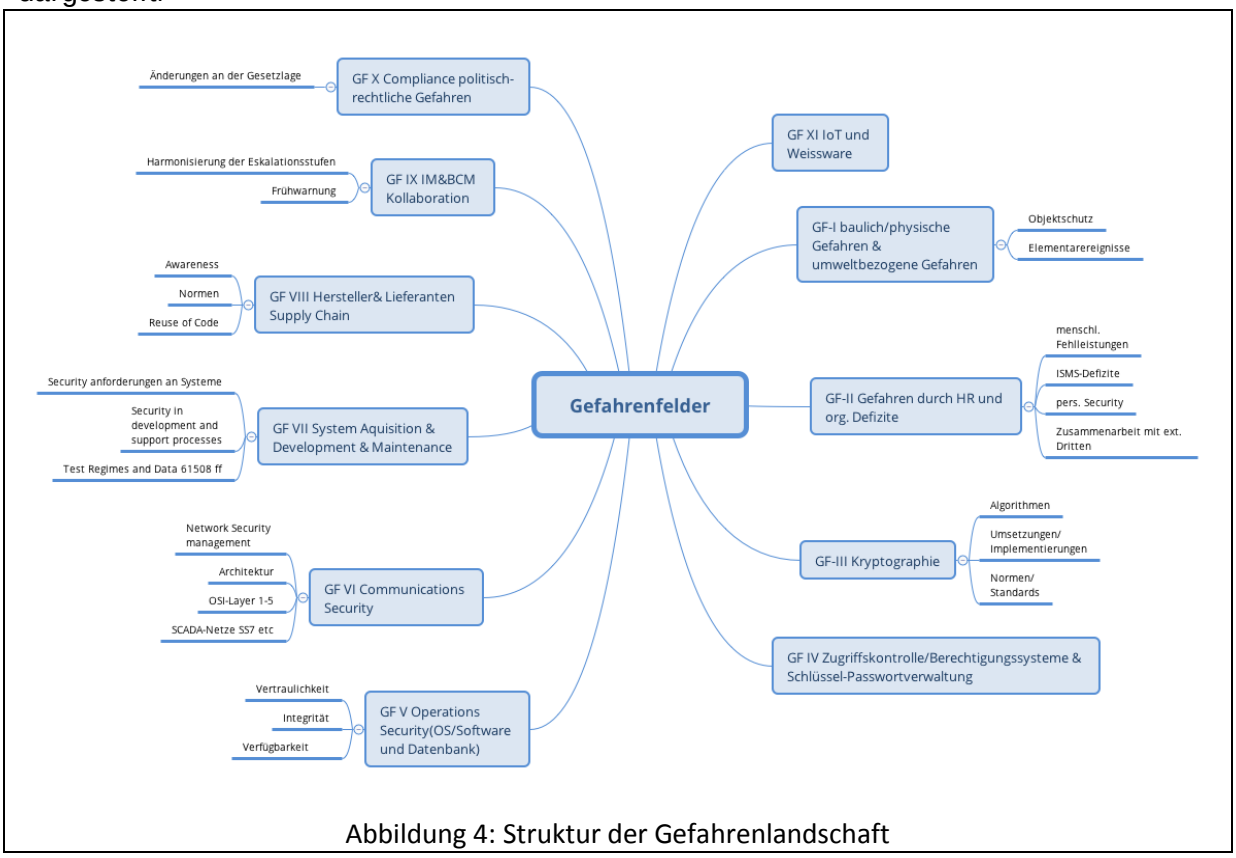


Abbildung 4: Struktur der Gefahrenlandschaft

6.2 Kurzbeschreibung der Gefahrenfelder

6.2.1 GEFAHRENFELD-I: BAULICH/PHYSISCHE GEFAHREN & UMWELTBEZOGENE GEFAHREN

Dieses Gefahrenfeld beschreibt im Wesentlichen die Herausforderungen durch technische Gefahren wie Brände oder sonstige technische Störungen, Anforderungen im Objektschutz, mögliche Defizite bei Infrastrukturen (Gebäuden), physische Gewalt gegen IKT-Einrichtungen sowie alle Umweltgefahren, die nach ÖNORM S2401 in:

- endogene/tektonische Gefahren (Erdbeben etc.)
- gravitatorische Gefahren (Erdrutsche und Muren etc.)
- klimatische Gefahren (Unwetter, Starkniederschlagereignisse oder auch Hochwasser etc.)
- sonstige Gefahren wie Epidemien

gegliedert sind.

6.2.2 GEFAHRENFELD-II: GEFAHREN DURCH HUMAN RESSOURCES UND ORGANISATORISCHE DEFIZITE

Dieses Gefahrenfeld beschreibt alle wesentlichen Herausforderungen, die sich mit menschlichen Fehlleistungen und organisatorischen Defiziten innerhalb und zwischen Organisationen beschäftigen. Adressiert werden insbesondere die Themen Sicherheitsbewusstsein für Informationssicherheit in der Gesamtheit aller Funktionen in einem Unternehmen inklusive der Managementsysteme.

6.2.3 GEFAHRENFELD-III: KRYPTOGRAPHIE & SOFTWARE & PROTOKOLLE

Dieses Gefahrenfeld beschreibt die kommenden bzw. bereits heute absehbaren Herausforderungen bei der Implementierung von kryptographischen Algorithmen zur Beherrschung von Vertraulichkeit und Integrität. Angesprochen werden hier absichtliche, eingebaute Schwachstellen in weit verbreiteten Protokollen genauso wie Probleme bei der Kombination von Hard- und Software, um einen definierten Sicherheitszustand erreichen zu können.

6.2.4 GEFAHRENFELD-IV: ZUGRIFFSKONTROLLE BERECHTIGUNGSSYSTEME & SCHLÜSSEL- UND PASSWORTVERWALTUNG

Dieses Gefahrenfeld beschäftigt sich mit der Entwicklung bzw. Weiterentwicklung der Implementierung von Zugriffskontrollsystemen, Aufbau und Implementierung von PKI-Infrastrukturen inklusive der sehr spezifischen TELKO-Problematiken, dass Leistungsmerkmale von TK-Anlagen nur bedingt wirksam unterbunden werden können, da aufgrund der technischen Entwicklungen eine Absicherung nur in Teilen möglich ist.

6.2.5 GEFAHRENFELD-V: OPERATIONS SECURITY

Dieses Gefahrenfeld ist eine sehr umfassende Beschreibung fast aller Probleme und Herausforderungen, die sich durch den Einsatz von Hard- und Software ergeben können. Speziell fokussiert dieses Gefahrenfeld daher auf die möglichen betrieblichen Gefahren, die sich primär durch bis dato nicht erkannte Vulnerabilitäten bei Hard- und Software und auch durch Fehlkonfigurationen ergeben können. Im Schwerpunkt also auf hauptsächlich

betriebliche Gefahren, mit denen Organisationen im täglichen Umgang mit der IKT konfrontiert sind.

6.2.6 GEFAHRENFELD-VI: COMMUNICATIONS SECURITY

Dieses Gefahrenfeld beschäftigt sich im Wesentlichen mit der Netzwerksicherheit inklusive der Verfügbarkeit und Integrität von Netzwerken.

6.2.7 GEFAHRENFELD-VII: SYSTEM AQUISITION & DEVELOPMENT & MAINTENANCE & DECOMMISSIONING

Dieses Gefahrenfeld beschäftigt sich im Kern mit den zum Teil stark optimierungsbedürftigen Securityaspekten im gesamten Life-Cycle von Hard-und Software inklusive des Ausscheidens von Hard- und Software aus dem laufenden Betrieb und den damit verbundenen Sicherheitsherausforderungen. Das Patch- und Änderungsmanagement inklusive der damit verbunden organisatorischen Herausforderungen stellen einen weiteren Schwerpunkt in diesem Gefahrenfeld dar.

6.2.8 GEFAHRENFELD-VIII: HERSTELLER& LIEFERANTEN SUPPLY CHAIN

Dieses Gefahrenfeld beschäftigt sich kurz zusammengefasst mit der gesamten Supply Chain Security. Besonderes Augenmerk wird auf die Themen Security Awareness bei den Herstellern und Lieferanten gelegt sowie auf die Abhängigkeit von singulären Lieferanten in speziellen Hard- und Softwaresegmenten.

6.2.9 GEFAHRENFELD-IX: IM&BCM KOLLABORATION

Dieses Gefahrenfeld beschäftigt sich mit den Herausforderungen im Incident Management, mit den Anforderungen an das Business Continuity Management und mit den künftigen Aufgabenstellungen in der Kollaboration mit anderen Branchen bis hin zu nationalen Behörden bei Cyber-Krisen.

6.2.10 GEFAHRENFELD-X: COMPLIANCE POLITISCH-RECHTLICHE GEFAHREN

Dieses Gefahrenfeld beschäftigt sich im Wesentlichen mit den zukünftigen normativ-rechtlichen Rahmenbedingungen und den damit verbundenen Chancen und Risiken für TELKOs und ISPs. Insbesondere die nationale und internationale Vernetzung in der Genese von neuen Rechtsvorschriften und Normen wird dabei adressiert.

6.2.11 GEFAHRENFELD-XI: IOT UND WEIßWARE

Dieses Gefahrenfeld beschreibt die kommenden betrieblichen Herausforderungen bei TELKOs und ISPs durch die Vernetzung vieler Endkundengeräte, insbesondere dann, wenn diese Geräte nur mehr IPv6 adressieren.

6.3 Aufbau des Gefahrenkatalogs

Der Gefahrenkatalog ist für alle 11 Gefahrenfelder gleich aufgebaut. Er gliedert sich wie folgt:

Gefahrenfeld-I baulich/physische Gefahren & umweltbezogene Gefahren				
Subkategorie	Nr.	Gefahren	Referenz	Prio 1-5
Gefahren, die durch Defizite im Objektschutz entstehen können	GF-I-01	Gefahr der Brandstiftung	ENISA-GL-4.1.7	
	GF-I-04	Gefahr einer Leitungsunterbrechung (durch Bauarbeiten o. dgl.)	ENISA-GL-4.1.15	
	GF-I-05	Gefahr einer Unterbrechung der Energieversorgung	ENISA-GL-4.1.16	
	GF-I-06	Eindringen in Sicherheitszonen	ISO-27002-11.1	
	GF-I-08	Großereignisse im Umfeld/Gefährdete Objekte/Nachbarn	BSI-IT-GS-G 0.5	
	GF-I-13	Gefahr unerkannter und unbefugter Zutritte zu schutzbedürftigen Räumen und Defizite bei Zutrittskontrollen (verlorene Schlüssel)	BSI-IT-GS-G 0.5	
	GF-I-19	Manipulation an Leitungen (inkl. Stromleitungen)	BSI-IT-GS-G 0.5	
	GF-I-23	Abhören von Telefongesprächen und Datenübertragungen	BSI-IT-GS-G 0.5	
	GF-I-24	Abhören von Räumen über TK-Endgeräte	BSI-IT-GS-G 0.5	

Tabelle 1: Aufbau des Gefahrenkatalogs

Die Referenzen verweisen auf die bereits bestehenden Gefahrenkataloge bei z. B. ENISA, oder beim BSI.

7. 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.

7.1 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 Verfügbarkeit von Kommunikationsnetzen oder –dienste" nach § 16a Abs 5 TKG 2003 wurden diskutiert. Für die Risikobetrachtungen ist es jedoch wichtig darzustellen, dass es einer skalierbaren und damit einer für alle TELKO und ISP 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 TELKOs und ISPs 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"[4] 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. krimine llen 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.

[4] TELKO und ISPs

7.2 Festlegung der Eintrittswahrscheinlichkeiten und Machbarkeit

7.2.1 TECHNISCHE GEBRECHEN UND NATURGEFAHREN

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

Tabelle 2: Bewertung der Eintrittswahrscheinlichkeit bei technischen Gefahren und Naturgefahren

7.2.2 FESTLEGUNG DER MACHBARKEIT; FÜR INTENTIONALE GEFAHREN

Machbarkeit Intentionale Gefahren			Bewertung Punkte
Eintritts-wahrscheinlichkeit	Verbale Beschreibung	Aufwand in Zeit und Know-how	
unwahrscheinlich	Sehr hoher Aufwand für die Tatausführung. Setzt Wissen voraus, das man sich durch sehr intensive Beschäftigung mit der Materie über einen längeren Zeitraum aneignen muss. Die Tat setzt auch voraus, dass man physische oder organisatorische IKT Barrieren unentdeckt überwinden kann. Eingesetzte Hilfsmittel zur Überwindung (Angriffsmethoden/Vektoren) sind bis dato unbekannt.	Wochen - Monate der Vorbereitung/ Expertenniveau	**1**
selten	Hoher Aufwand für die Tatausführung. Setzt Wissen voraus, das man sich durch intensive Beschäftigung mit der Materie aneignen kann. Die Tat setzt voraus, dass man organisatorische IKT Barrieren (auch soziale Kenntnisse) unentdeckt überwindet. Es wird ein Mix aus bekannten und unbekannten Angriffsmethoden/Vektoren verwendet. Information über Infrastruktur und Zugriffsmöglichkeiten darauf. Angriffe auf die physische Infrastruktur Layer 1 (LWL, Koax, Cu, Funk).	Wochen der Vorbereitung - spezielle Fachkenntnisse werden vorausgesetzt	**2**
gelegentlich	Überschaubarer Aufwand für die Tatausführung. Das Ziel hat subjektiv eine gewisse Attraktivität. Die Tat setzt voraus, dass bekannte Schwachstellen in organisatorischen IKT Barrieren mit bekannten Hilfsmitteln überwunden werden müssen. (Keine Automatisation der Angriffe/Vektoren)	Tage der Vorbereitung- Fachkenntnisse werden vorausgesetzt	**3**
öfters	Geringer Aufwand für die Tatausführung. Das Ziel hat eine subjektiv hohe Attraktivität. Die Tat setzt voraus, dass bekannte Schwachstellen in IKT-basierten Barrieren mit vorhandenen Werkzeugen automatisiert überwunden werden können.	Wenige Tage der Vorbereitung werden vorausgesetzt.	**4**
häufig	Sehr geringer Aufwand für die Tatausführung notwendig. Es reicht, bestehende Hilfsmittel/Werkzeuge für die Überwindung von IKT-Barrieren einzusetzen, um erfolgreich zu sein	Es stehen bereits anpassbare Werkzeuge bzw. Werkzeugkisten zur Verfügung. Die Tat kann von interessierten Laien begangen werden.	**5**
	Aufwand wird auch immer finanziell verstanden		

Tabelle 3: Bewertung der „Eintrittswahrscheinlichkeit" intentionaler Gefahren

Eine Besonderheit der IKT Risikoanalyse ist, dass bei manchen Gefahren eine Eintrittswahrscheinlichkeit mit den hier abgeschätzten Häufigkeiten nur bedingt sinnvoll ist, da diese Gefahren in kurzen Intervallen „ständig" beschrieben werden können. Es wurde daher eine zusätzliche Visualisierung von Risiken gewählt, die losgelöst von den hier angenommenen Eintrittswahrscheinlichkeiten eine reine Auswirkungsdimension aufweist, bei der im Vergleich zu den anderen Gefahren mit der hohen Periodizität der Vorkommnisse argumentiert werden kann.

Für die Bewertung der Auswirkungsdimensionen wurden die wesentlichen Eigenschaften:

- Verlust der Verfügbarkeit
- Verlust der Integrität
- Verlust der Vertraulichkeit herangezogen.

Parallel dazu wurde versucht, eine monetäre Größenordnung der Schadensdimensionen zu formulieren, wobei hier der abgeschätzte Primärschaden im Vordergrund steht. Selbstverständlich kann es sich hier nur um eine erste Näherung handeln, die in einer realen Situation eingehend analysiert werden muss.
Mit Blick auf die bereits beschriebene Vergleichbarkeit bei den unterschiedlichen Betreibern wurde für die Bewertung der Verfügbarkeit das Produkt aus betroffenen Kunden mal einer Ausfallszeit als ein abgestuftes Schadensausmaß herangezogen bzw. definiert. Mit dieser Vorgehensweise sind mehrere Schadensbilder beschreibbar. Kurzzeitige Ausfälle mit vielen betroffenen Kunden aber auch andere Extreme wie längerfristiger Ausfälle von wenigen Kunden. In Summe können hier mehrere Szenarien in einer allgemein gültigen Form für alle Betreibergrößen gleich beschrieben werden.

7.3 Bewertungskriterien der Auswirkungsdimensionen

Bewertung der Auswirkungsdimension					
Auswirkung	Verbale Beschreibung qualitativ			Beschreibung quantitativ	Bewertung Punkte
	Verfügbarkeit	Vertraulichkeit	Integrität		
gering	Ereignis betrifft 0-2%h. Keine Notrufe/verfügbarkeitskritische Services betroffen. Performanceeinbußen möglich	kein/ geringer Imageschaden	Integrität aller Services unberührt. Genutze eingesetzte Sicherungs-Technik weiterhin uneingeschränkt nutzbar	Primärschaden < 0,1% Jahresumsatz	**1**
mittel	Ereignis betrifft 2-80%h aller Kunden. Keine Notrufe/verfügbarkeitskritische Services betroffen. Spürbare Performanceeinbußen bei Teilen des Netzes/Services/Applikationen	Schützenswerte Daten wurden ungewollt veröffentlicht. Wiederherstellung der Vertraulichkeit gering. Geringer Imageschaden	Netze/Services/Applikationen werden durch (gezielte) Veränderungen kurzzeitig zu Absturz/Dysfunktion gebracht. Wiederherstellungsaufwand gering. Eingesetzte Sicherungs-Technik grundsätzlich weiterhin nutzbar	Primärschaden 0,1-2% Jahresumsatz	**2**
hoch	Ereignis betrifft 80-360%h aller Kunden. Keine Notrufe/Notrufträger lokal betroffen/verfügbarkeitskritische Services betroffen. Erhebliche Performanceeinbußen bei Teilen des Netzes/Services/Applikationen	Schützenswerte Daten wurden gezielt und in erheblichem Umfang veröffentlicht. Nutzung der Daten wird Einzeltätern zugeschrieben. Wiederherstellung der Vertraulichkeit hoch. Hoher Imageschaden.	Netze/Services/Applikationen werden durch (gezielte) Veränderungen nachhaltig zu Absturz/Dysfunktion gebracht. Wiederherstellungsaufwand hoch. Eingesetzte Sicherungs-Technik muss angepasst werden. Keine grundsätzliche Änderung von Architekturen notwendig	Primärschaden 2-5% Jahresumsatz, DSGVO (4% Jahresumsatz)	**3**

Bewertung der Auswirkungsdimension					
Auswirkung	Verbale Beschreibung qualitativ			Beschreibung quantitativ	Bewertung Punkte
	Verfügbarkeit	Vertraulichkeit	Integrität		
sehr hoch	Ereignis betrifft 360-1920%h aller Kunden. Notrufe/Notrufträger auf Bundeslandebene betroffen/verfügbarkeitskritische Services betroffen. Erhebliche Performanceeinbußen bei allen Netzes/Services/Applikationen	(wie hoch aber zusätzlich) Daten wurden gezielt veröffentlicht, mit dem Ziel die persönliche Sicherheit zu gefährden. Nutzung der Daten wird kriminellen Gruppierungen zugeschrieben. Wiederherstellung der Vertraulichkeit erheblich. Sehr hoher Imageschaden.	Netze/Services/Applikationen müssen aufgrund der Ereignisse grundsätzlich überarbeitet werden. Wiederherstellungsaufwand sehr hoch. Eingesetzte Sicherungs-Technik muss systematisch angepasst werden. Keine grundsätzliche Änderung von Architekturen notwendig. Anpassung rechtlich/normative Änderungen werden notwendig.	Primärschaden 5-10% Jahresumsatz, Kapitalmaßnahmen durch den jur. Eigentümer erforderlich	**4**
katastrophal	Ereignis betrifft >1920%h aller Kunden. Notrufe/Notrufträger flächendeckend betroffen/verfügbarkeits-kritische Services betroffen. Performanceeinbußen bei Teilen des Netzes/Services/Applikationen sind so hoch, dass diese de facto nicht genutzt werden können	(wie hoch aber zusätzlich) Daten wurden gezielt über Jahre hinweg unbemerkt, mit dem Ziel die persönliche Sicherheit zu gefährden abgegriffen. Nutzung der Daten wird staatlichen Organisationen zugeschrieben. Wiederherstellung der Vertraulichkeit erheblich. Katastrophaler Imageschaden.	Netze/Services/Applikationen müssen aufgrund der Ereignisse komplett re-designed werden. Schwer bis kaum abzuschätzender Wiederherstellungsaufwand, da komplett neue Systeme eingeführt werden müssen. Eingesetzte Sicherungs-Technik muss systematisch angepasst werden. Es ist eine grundsätzliche Änderung der Architektur notwendig. Gesetzliche Anpassungen ziehen enorme Veränderungen nach sich. Einsatz gezielter Methoden zur Fremdkontrolle der Systeme	Primärschaden >10% Jahresumsatz, Kapitalmaßnahmen durch den jur. Eigentümer erforderlich	**5**
Für die Bewertung der negativen „Auswirkung“ wird ein logisches „oder“ herangezogen und das für das jeweilige Unternehmen/Org**anisation wichtigste Kriterium ausgewählt**					
%h = (relativer Anteil betroffene Kunden) * (Ausfall in Stunden) [%h]					
Unter Sicherungs-Technik wird ein Überbegriff verstanden der auch kryptografische Techniken einschließt					

Tabelle 4: Bewertung der Schadensdimension

7.4 Risikobewertungsprozess

In Summen wurden 487 Gefahren in mehreren Arbeitsworkshops zu Risiken bewertet. Dazu wurden folgende Schritte abgearbeitet:

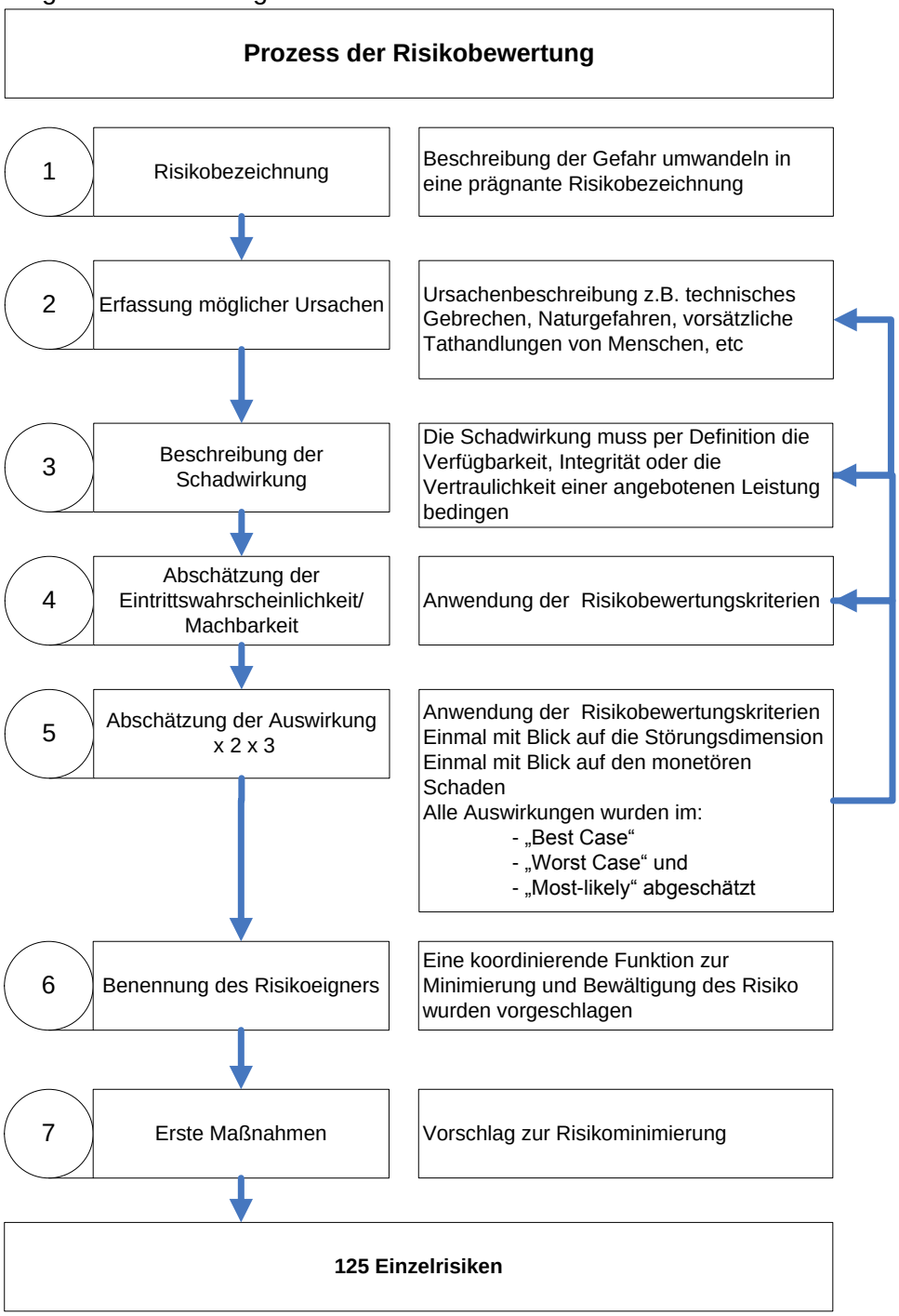


Abbildung 5: Prozess der Risikobewertung

8. Ergebnisdarstellung der Einzelrisiken

Die Einzelrisiken wurden in einem eigenen Risikokatalog zusammengestellt. Exemplarisch wird hier die Struktur dargestellt:

A	B	C	D	E	F	G	H
Nr	**Risikobezeichnung**	**Ursachen**	**Wirkung**	**Wahr-scheinlichkeit**	**Höhe der Auswirkung**	**Risiko von**	**Risiko bis**
1	Sonnensturm	Naturgefahr	Erhebliche flächendeckende physische Zerstörungen von IKT-Infrastruktur	1	5	5	5
2	IKT-Leitungsunterbrechung in Verteilnetz	Techn. Gebrechen durch Baggerangriff, unsachgemäße Bauarbeiten	Erhebliche Störungen von 0 bis 80 % h	5	1 - 2	5	10

Tabelle 5: Teil 1 der Einzelrisikoerfassungstabelle

Fortsetzung der Tabelle

I	J	K	L	M	N	O
Risiko-Owner	**Schadens-ausmaß (€) VON**	**Schadens-ausmaß (€) ERWARTUNGS-WERT**	**Schadens-ausmaß (€) BIS**	**Maßnahmen zur Risikobewältigung**	**Anmerkungen; Maßnahmen-vorschläge**	**Kategorie**
TELKO	1	3	5	Forschung über Schadenswirkung bei Sonnenstürmen / Frühwarnsystem durch die ZAMG initiert	I-38,	Naturgefahr
ISPs	0	0	0	ONR - S2411 ab 2019 anwenden	I-04,	Technik und Infrastruktur

Tabelle 6: Teil 2 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 10-20 Jahr im „Best Case" im „Worst Case" kommt diese Gefahr einmal in 5 Jahren vor.
- Spalte F, Bewertung der Auswirkungsdimension nach den Bewertungskriterien (auch hier können Intervalle angegeben werden z. B 1-2, gleichbedeutend einem Ereignis

der Verfügbarkeit von 0-2%h bis hin zu 2-80%h, sofern die Verfügbarkeit beschrieben wurde).

- 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 monetären Impacts im „Best-Case"-Fall dar
- Spalte K, stellt eine erste Abschätzung des monetären Impacts im „Most-Likely"-Fall dar
- Spalte L, stellt eine erste Abschätzung des monetären Impacts im „Worst-Case"-Fall dar
- Spalte M, beschreibt entweder direkt Maßnahmen zur Risikominderung oder gibt Empfehlungen wie z. B. bei Nummer 2, ab 2019 die ONR S2411, „Arbeitstitel Methoden zur zerstörungsfreien Vorerkundung und Risikominimierung von alten und historischen Hinterlassenschaften und technischer Infrastrukturen im Boden zu beachten.
- Spalte N, verweist auf die Gefahrennummer nach römisch I= Gefahrenfeld I und laufender Nummer im jeweiligen Gefahrenfeld
- Spalte O, ordnet das Risiko einer Risikokategorie zu. Hier im konkreten Fall einmal zu Naturgefahren ein einem der Risikokategorie Technik und Infrastruktur.

Die Ergebnisse der Risikobewertung aller 487 Gefahren wurden im „Best Case" im „Worst Case" und im „Most-Likely"-Fall bewertet und in **einer** Risikomatrix zusammengestellt. Der Einfachheit halber werden hier nur die „Worst-Case"-Betrachtungen (Worst-Case-Matrix) abgebildet.

9. Ergebnisdarstellung der Aggregationsrisiken

9.1 Aggregationsprozess

Die 125 Einzelrisiken wurden aus dem Gefahrenkatalog abgeleitet. Um die Einzelrisiken auf ein überschaubares Maß zu reduzieren, wurden die Einzelrisiken in Risikokategorien eingeordnet. Es wurden folgende 12 Risikokategorien definiert:

1. Beschaffung
2. Betrieb
3. Crypto und Zugriffskontrolle
4. Design und Architektur
5. Eskalation und Kommunikation
6. Hard- und Software
7. Human Factors
8. Intentionale Gefahren
9. Naturgefahr
10. Normung und Recht
11. Organisatorische Sicherheit
12. Technik und Infrastruktur

Diese Kategorisierung wurde in einem ersten Schritt dazu benutzt, einen ersten Aggregationsvorschlag zu erarbeiten. Die Aggregationsrisiken wurden anschließend 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 wurde ein Risikoeigner formuliert und Maßnahmen zur Risikominimierung als Vorschlag erarbeitet.

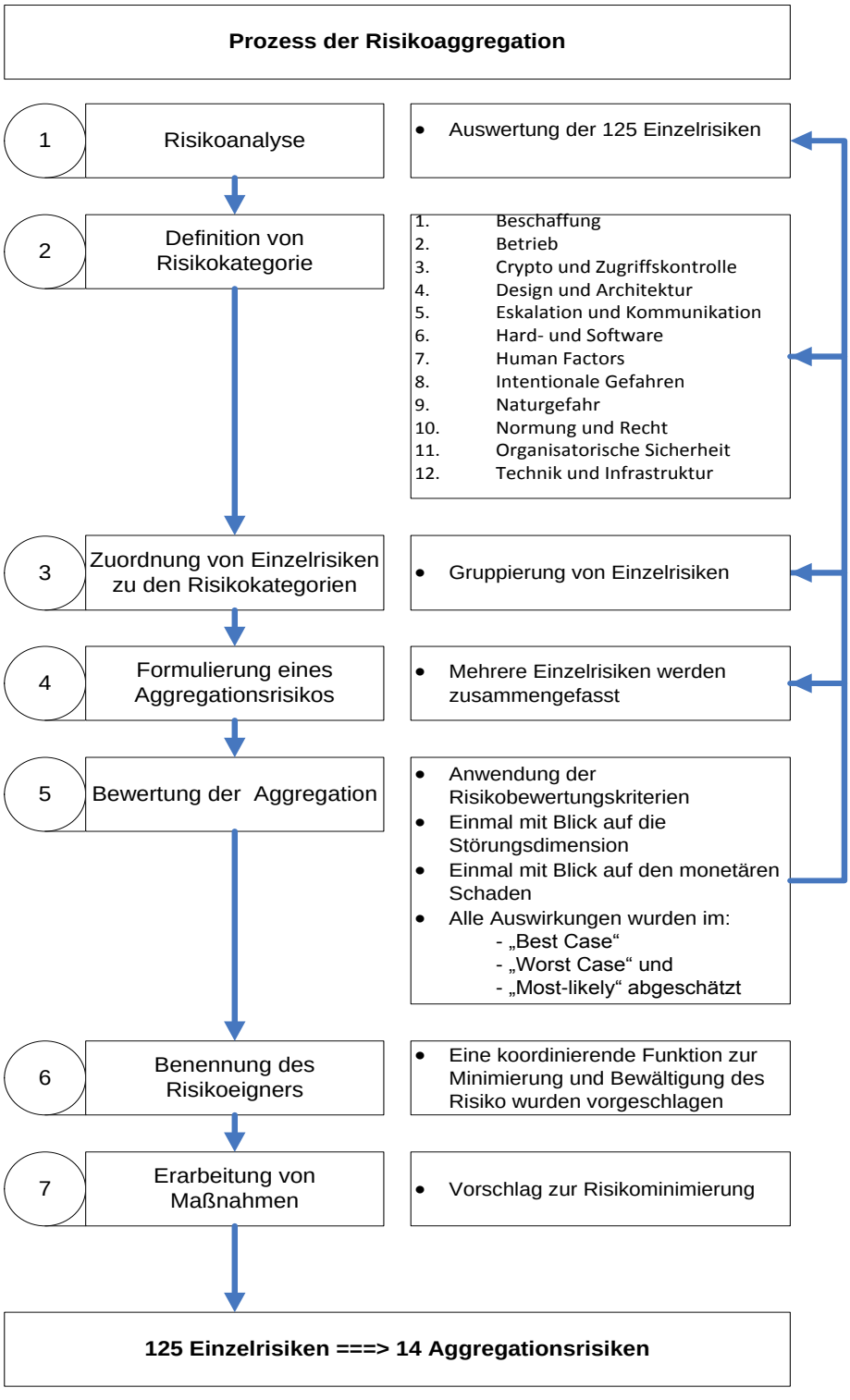


Abbildung 6: Risikoaggregationsprozess

9.2 Aggregationsrisikomatrix im „Worst Case“

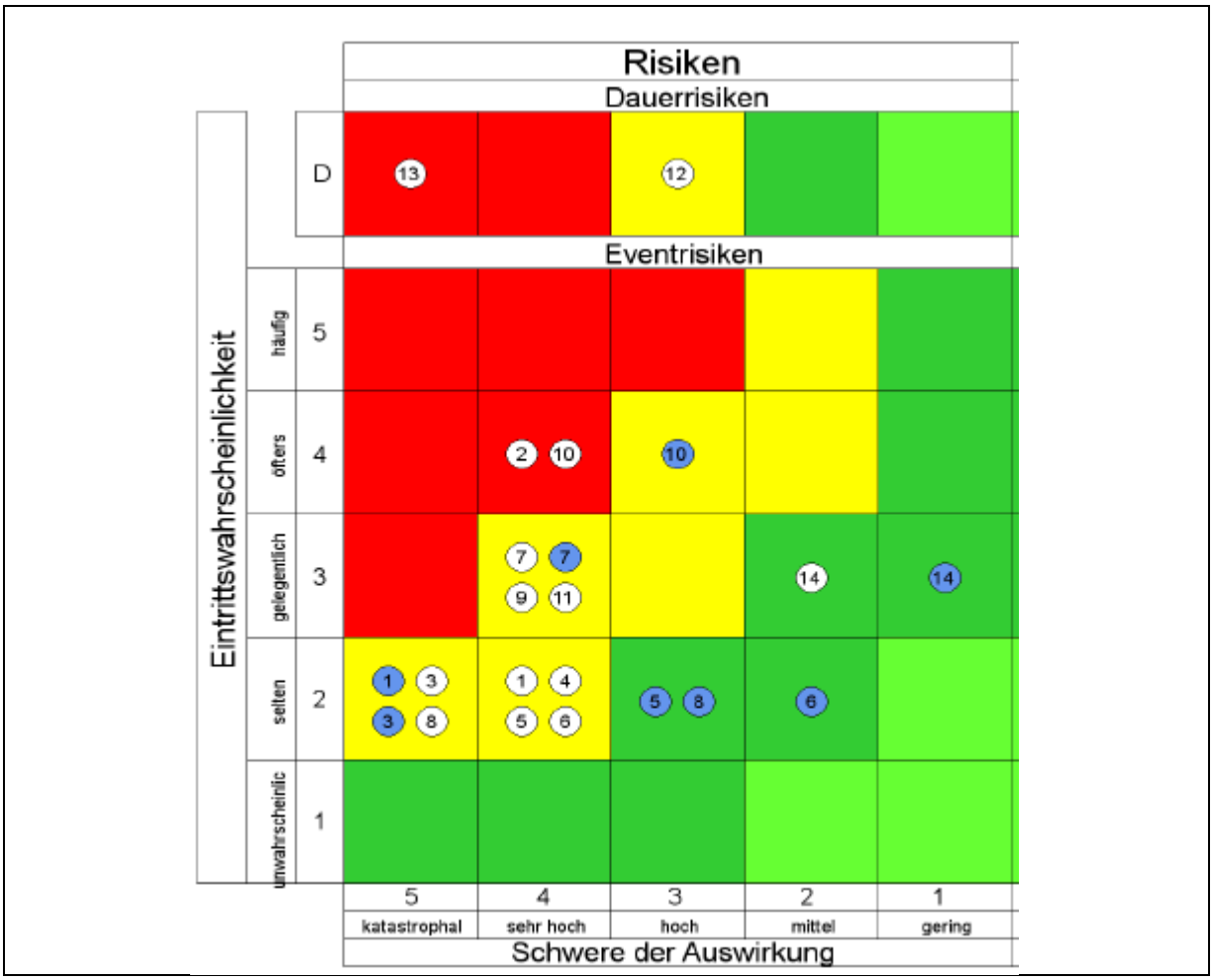


Abbildung 7: Aggregationsmatrix im "Worst Case"

Risiken in weißen Kreisen sind nach Verfügbarkeit, Integrität und Vertraulichkeit bewertet, die blauen Risiken sind mit gleicher Ordnungsnummer nach monetären Gesichtspunkten bewertet.

9.3 Aggregationsrisikomatrix im „Most-likely“

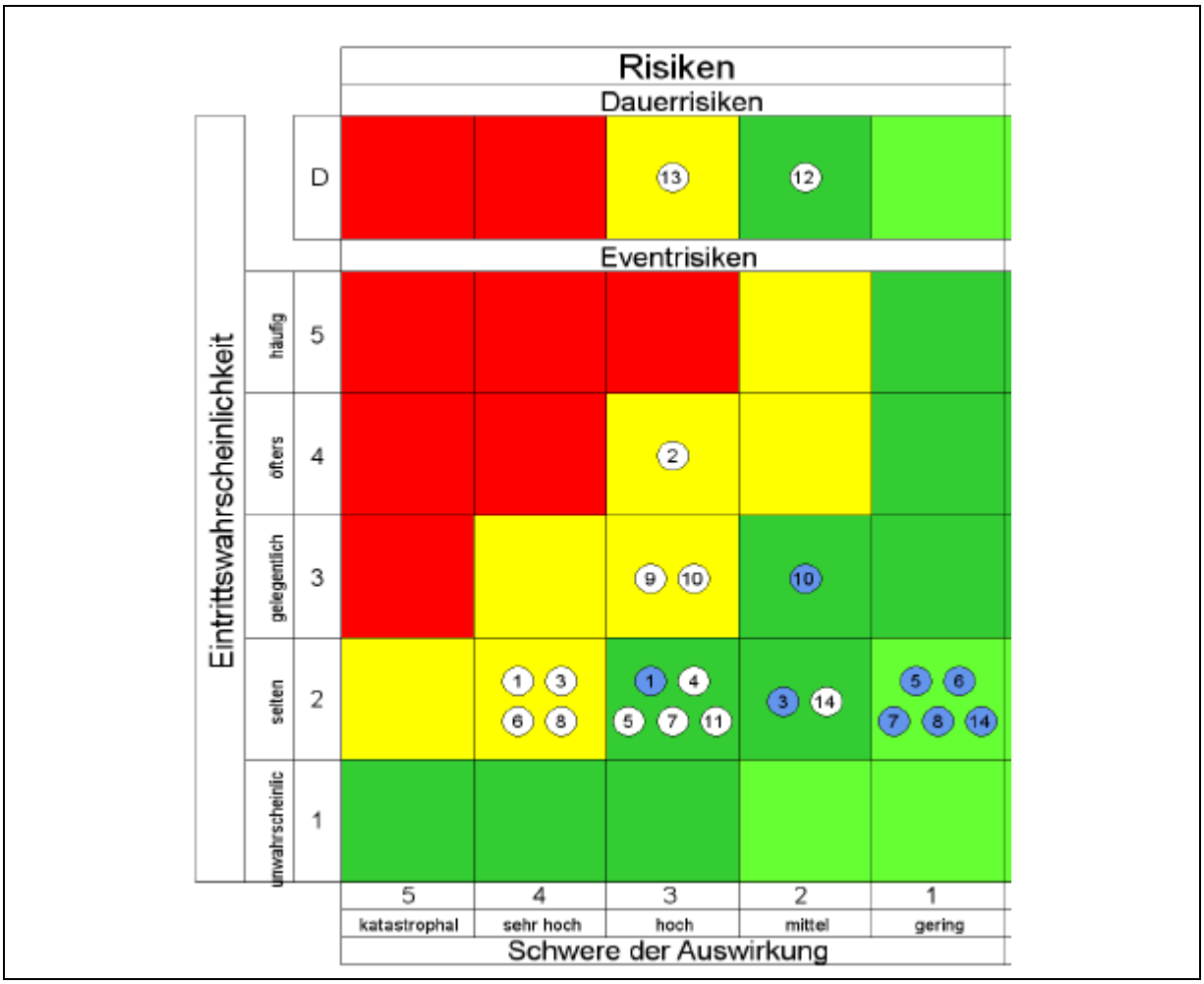


Abbildung 8: Aggregationsmatrix im "Most-likely"

Risiken in weißen Kreisen sind nach Verfügbarkeit, Integrität und Vertraulichkeit bewertet, die blauen Risiken sind mit gleicher Ordnungsnummer nach monetären Gesichtspunkten bewertet.

9.4 Aggregationsrisikomatrix im „Best Case“

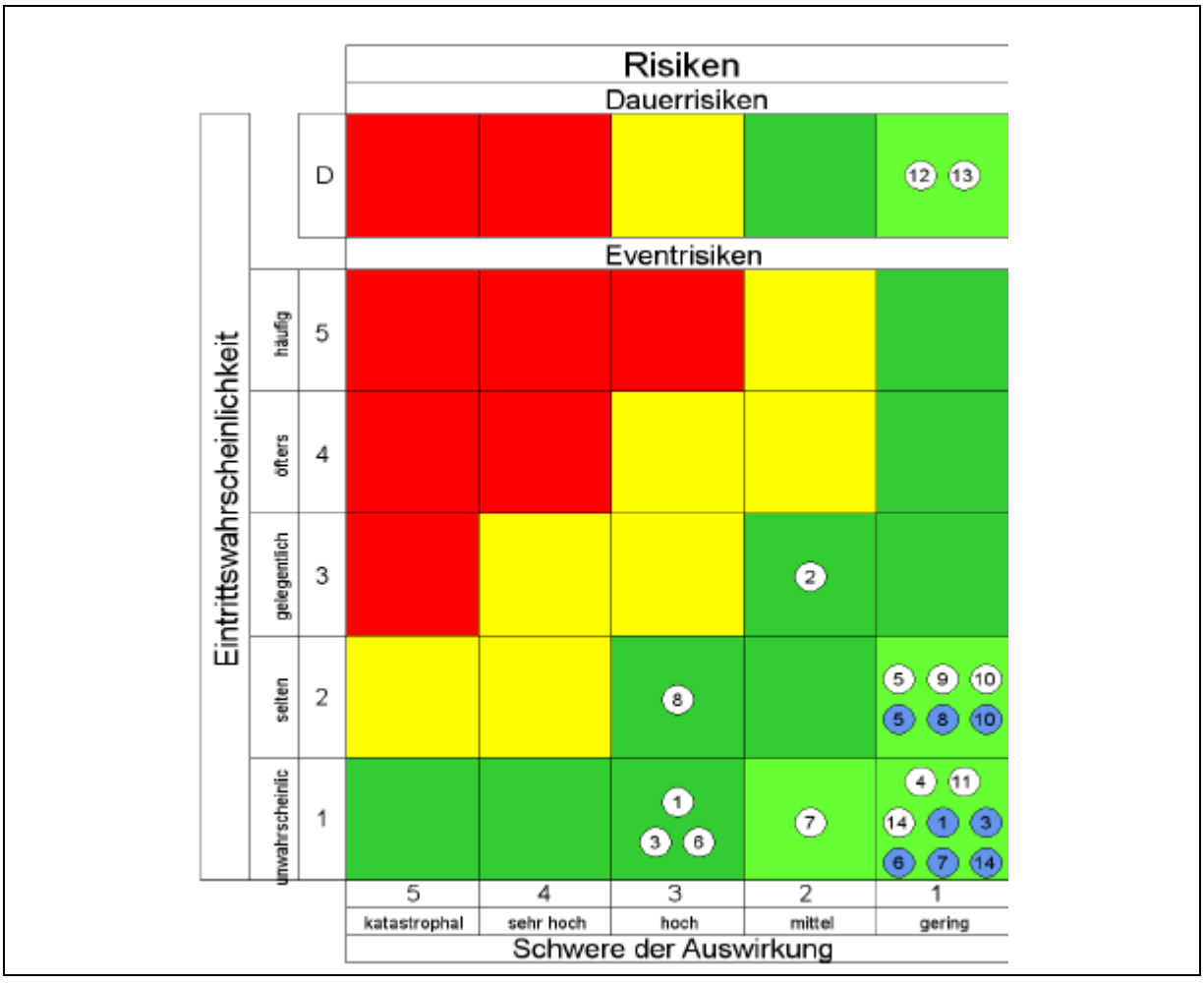


Abbildung 9: Aggregationsmatrix im "Best Case"

Risiken in weißen Kreisen sind nach Verfügbarkeit, Integrität und Vertraulichkeit bewertet, die blauen Risiken sind mit gleicher Ordnungsnummer nach monetären Gesichtspunkten bewertet.

9.5 Auswertung der Risikokategorien

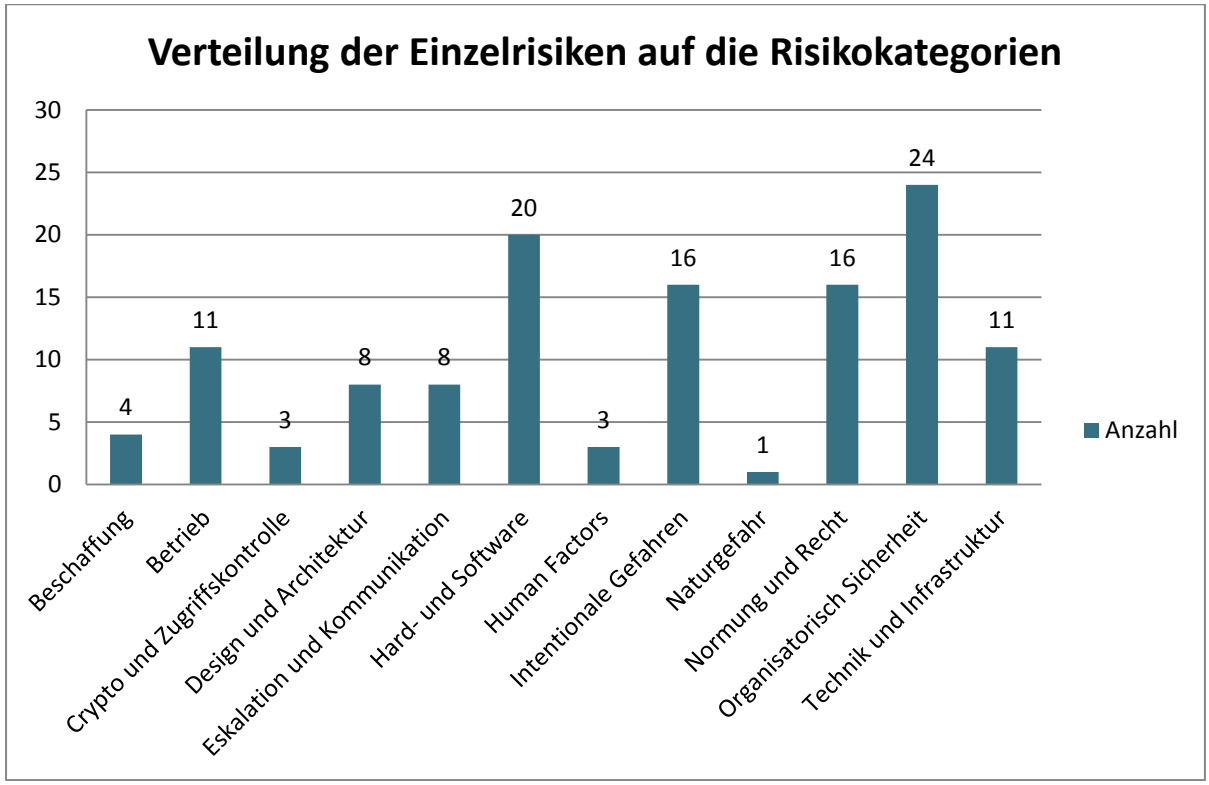


Abbildung 10: Darstellung der Verteilung der Risikokategorien

Teil IV Maßnahmen & Empfehlungen

10. Empfehlungen

Die nachfolgenden Empfehlungen leiten sich aus mehreren Perspektiven ab und fassen die Ergebnisse der Diskussionen in den elf Expertenworkshops im Jahr 2017 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. 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) zugordnet werden können, lässt sich wie folgt beschreiben. Es werden Unternehmen in Österreich als „strategisch wichtige Unternehmen gemäß APCIP (vgl. dazu Kapitel 5.1)“, 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 BM.I/BKA bereits via Information an die Geschäftsleitung über ihren Status informiert bzw. werden laufend informiert.
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 in der Expertengruppe der RTR-IKT-Branchenrisikoanalyse festgelegt.

Unter diesen Betreibern (SysB) versteht man - in Anlehnung an die voraussichtlichen Grenzwerte des Bundesgesetzes zur Cybersicherheit - diejenigen Unternehmen der IKT-Branche, welche folgende Dienste in Quantität für mehr als 1% der österreichischen Bevölkerung oder mehr als 5 % der jeweiligen Bundesländerbevölkerung anbieten:

- Telefonie/Festnetz
- Telefonie/Mobilnetz
- Internetzugang/Festnetz
- Internetzugang/Mobilnetz

Die Schwellwerte für systemrelevante Betreiber (1 % bundesweit, 5 % in einem Bundesland) werden den Ausführungsbestimmungen zum NIS-Gesetz bezüglich der Festlegung der Betreiber wesentlicher Dienste angepasst.

Empfehlungen an die relevanten Betreiber (SysB) 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 Lenkungsausschuss der RTR-IKT-Branchenrisikoanalyse den Umsetzungsstand darstellen und ggfs. Anpassungen vorschlagen.

10.2 Priorisierung und Zeithorizonte der Empfehlungen

Im Rahmen der Abstimmungsarbeiten zum Bericht wurde vereinbart, dass es keine Korrelation der Prioritäten der Empfehlungen mit einem definierten Umsetzungszeitraum 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
- Priorität 2
- Priorität 3

Für den Umsetzungshorizont (UH), wurden ebenfalls 3 Stufen gebildet:

- UH I, kurzfristig, Umsetzung kann innerhalb von 2 Jahren erfolgen
- UH II, mittelfristig, Umsetzung kann innerhalb von 2-5 Jahren erfolgen
- UH III, langfristig, eine Umsetzung wird voraussichtlich mehr als 5 Jahren benötigen

In einem möglichen Folgeprozess sollten die mit den erarbeiteten Empfehlungen verbundenen finanziellen und personellen Ressourcen identifiziert und abgestimmt werden. Dieser Prozess legt:

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

Inwieweit die Empfehlung für welche Gruppe an Organisationen und Unternehmen relevant sind, muss in einer gesonderten Signifikanzprüfung erfolgen. Im Rahmen dieses ersten Berichts wurde hierzu lediglich ein Vorschlag erarbeitet.

10.3 Übersicht der Empfehlungen

Aus den 12 Risikokategorien wurden 37 Empfehlungen formuliert.

Risikokategorien	Empfehlungen
1. Beschaffung 2. Betrieb 3. Crypto und Zugriffskontrolle 4. Design und Architektur 5. Eskalation und Kommunikation 6. Hard- und Software 7. Human Factors 8. Intentionale Gefahren 9. Naturgefahr 10. Normung und Recht 11. Organisatorische Sicherheit 12. Technik und Infrastruktur	» Eskalation und Kommunikation » Betrieb » Autorisierung/ Zugriffskontrolle » Beschaffung » Design und Architektur » Human Factors » Naturgefahren » Normung und Recht » Organisatorische Sicherheit

Diese verteilen sich auf folgende Risikokategorien wie nachstehend abgebildet:

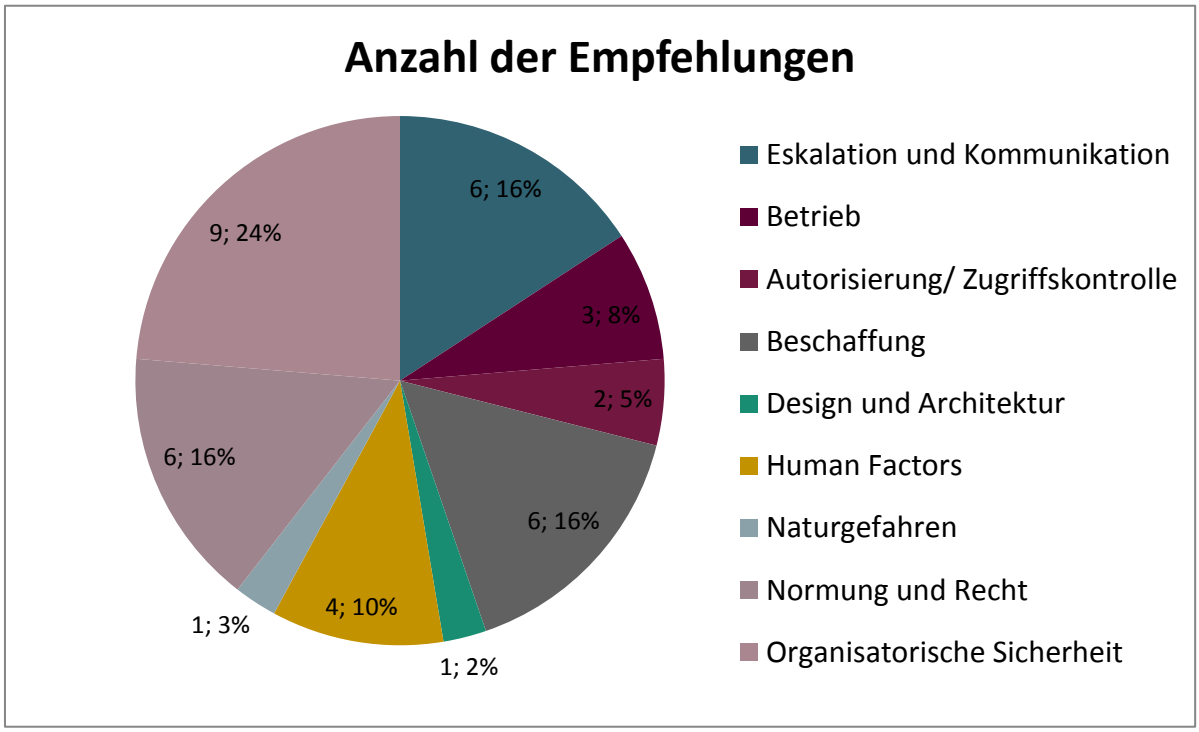


Abbildung 11: Verteilung der Empfehlungen auf die Risikokategorien

Abkürzungsverzeichnis

Abkürzungen	Beschreibung
APCIP	Österreichisches Programm zum Schutz kritischer Infrastrukturen
APT	Advanced Persistent Threat
BCM	Business Continuity Management
BKA	Bundeskanzleramt
BM.I	Bundesministerium für Inneres
BSI	Bundesamt für Informationssicherheit in Deutschland
CERT	Computer Emergency Response Team
CPE	Customer Premises Equipment
CSP	Cybersecurity Platform
(D) DOS	Distributed Denial of Service
ENISA	Europäische Agentur für Informationssicherheit
EPCIP	Europäisches Programm „Schutz Kritischer Infrastrukturen“
IM	Incident Management
IoT	Internet of Things Produkte
IS	Internetservices
ISMS	Informationssicherheitsmanagementsystem
ISO	International abgestimmte Norm
ISP	Internetserviceprovider
ISPA	Interessensvereinigung der Internetserviceanbieter Österreichs
KI	Kritische Infrastrukturen
KRITIS	Kritische Infrastrukturen
LSA	Lenkungsausschuss
NIS	Netz- und Informationssicherheit in der Union
ONR	Österreichische Normenregel
OS	In der Regel Betriebssysteme
ÖSCS	Österreichische Strategie zur Cybersicherheit
PDCA	Plan Do Check Act
PKI	Public Key Infrastructure
PPP-Prozess	Private Public Partnership
SKKM	Staatliche Krisen und Katastrophenmanagement
TELKO	Telekommunikationsprovider
TK-Anlagen	Telekommunikationsanlagen
USV	Umfassende Sicherheitsvorsorge

Quellenverzeichnis

- Lit.RTR-01, Schwachstelle im Mobilfunknetz: Kriminelle Hacker räumen Konten leer: http://www.sueddeutsche.de/digital/it-sicherheit-schwachstelle-im-mobilfunknetz-kriminelle-hacker-raeumen-konten-leer-1.3486504
- Lit.RTR-02, The Fall of SS7 - How Can the Critical Security Controls Help?: https://www.sans.org/reading-room/whitepapers/critical/fall-ss7-critical-security-controls-help-36225

  Lit.RTR-03, Netzsicherheit – Cybersicherheitsgesetz: https://www.rtr.at/de/inf/TKForum2016/Praesentation_NIS-Richtlinie_und_Netzsicherheit.pdf
- Lit.RTR-04, 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.RTR-05, Security Profiles ISPA Arbeitsgruppe Security ‚Sicherheitskonzept (Mustervorlage) für Betreiber öffentlicher Kommunikationsnetze und –dienste: https://www.rtr.at/tr/inf/Workshop10102013/30053_Mustervorlage_Sicherheitskonzept.pdf
- Lit.RTR-06, Study on Mobile Device Security: https://www.dhs.gov/sites/default/files/publications/DHS%20Study%20on%20Mobile%20Device%20Security%20-%20April%202017-FINAL.pdf
- Lit.RTR-07, Cyber-Risiken Österreich 2016: https://kuratorium-sicheres-oesterreich.at/wp-content/uploads/2017/09/KS%C3%96-Risikobericht-2016-Folder.pdf
- Lit.RTR-08, Report Cyber-Risikomatrix: https://kuratorium-sicheres-oesterreich.at/wp-content/uploads/2015/02/Cyberrisikoanalyse.pdf
- Lit.RTR-09, Assessing Threats to Mobile Devices & Infrastructure - The Mobile Threat Catalogue: https://csrc.nist.gov/csrc/media/publications/nistir/8144/draft/documents/nistir8144_draft.pdf
- Lit.RTR-10, Digitaler Stillstand - Die Verletzlichkeit der digital vernetzten Gesellschaft: http://www.herbert.saurugg.net/2017/blog/vernetzung-und-komplexitaet/digitaler-stillstand
- Lit.RTR-11, Critical Security Controls V6.0 CIS TOP 20: https://www.sans.org/media/critical-security-controls/critical-controls-poster-2016.pdf
- Lit.RTR-12, 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.RTR-13, Annual Incident Reports 2015 - Analysis of Article 13a annual incident reports in the telecom sector: https://www.enisa.europa.eu/publications/annual-incident-reports-2015/at_download/fullReport

» Lit.RTR-14, Guideline on Threats and Assets - Technical guidance on threats and assets in Article 13a: https://www.enisa.europa.eu/publications/technical-guideline-on-threats-and-assets

» Lit.RTR-15, SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY Information and network security – Security management: https://www.itu.int/rec/T-REC-X.1051-200407-S/en

» Lit.RTR-16, SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY Telecommunication security: https://www.itu.int/rec/T-REC-X.1055-200811-I

» Lit.RTR-17, 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.RTR-18, Extremszenario - Physiker warnen vor Super-Sonnensturm: http://www.spiegel.de/wissenschaft/weltall/sonnenstuerme-forscher-warnen-vor-katastrophalen-stromausfaellen-a-840859.html

» Lit.RTR-19, Bundesgesetz über die Organisation der Sicherheitsverwaltung und die Ausübung der Sicherheitspolizei (Sicherheitspolizeigesetz – SPG): https://www.jusline.at/gesetz/spg

» Lit.RTR-20, Bundesgesetz, mit dem ein Telekommunikationsgesetz erlassen wird (Telekommunikationsgesetz 2003 –TKG 2003): https://www.rtr.at/de/tk/TKG2003

» Lit.RTR-21, 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.RTR-22, Cybersecurity Act https://sso.agc.gov.sg/Acts-Supp/9-2018/Published/20180312?DocDate=20180312

» Lit.RTR-23, 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