INFRA PROTECT

Rundfunk & Telekom
Regulierungs-GmbH

Bericht

IKT Branchen Risikoanalyse

Version 3.0-2021
RTR-WHITE-VERSION

RTR

Auftraggeber: RTR GmbH	Gesamtzahl Seiten: 52
Aufgabensteller: Mag. U. Latzenhofer	Anzahl Tabellen: 9
Studienkennziffer: entfällt	Anzahl Abbildungen: 19

Wien, 01.04.2021

Koordinierender Verfasser: DI Wolfgang Czerni, MBA

Kurzfassung

Der vorliegende Bericht fasst die Ergebnisse der Version 3.0-2020 der RTR-IKT-Branchenrisikoanalyse im Zeitraum von März 2019 bis November 2020 zusammen. Im Wesentlichen werden vier Schwerpunkte beschrieben.

Im Teil I werden die Methodik und Vorgehensweise, kurz wiederholend, zur Version 1.0 dargestellt. Teil II fasst die veränderten Rahmenbedingungen für den hier dargestellten Risikomanagementprozess zusammen. Insbesondere mit den im Vergleich zu den Vorjahren mit der Verabschiedung der „Digitalstrategie der Europäischen Kommission[1]“ sowie mit den Harmonisierungsanforderungen der „European Union Agency for Cybersecurity ENISA“, der ENISA Threat Landscape for 5G Networks[2], der Empfehlung (EU) 2019/534 der Kommission betreffend Cybersicherheit der 5G-Netze[3] sowie der daraus resultierenden EU Toolbox of risk mitigating measures[4] deutlich intensivierten Aktivitäten auf EU-Ebene wurden wesentliche Inputs im Rahmen der Aktualisierung geliefert. Parallel dazu wurden auch Beiträge zu nationalen Gesetzen und Vorschriften erarbeitet bzw. aus Sicht einer Gefahrenidentifikation und Bewertung analysiert. Hier wird der Kontext zu den Fact-Sheets[5] 08/2019 der NISV[6] und zur Umsetzung der TK-NSiV 2020[7] genannt. Eine, mit Blick auf die Aufträge seitens des Lenkungsausschusses, wesentliche Neuerung ist die begonnene Kooperation mit der Energiewirtschaft.
Teil III widmet sich der Darstellung und Diskussion der wesentlichen Ergebnisse wie Gefahrenkataloge, Einzel- und Aggregationsrisiken und Einarbeitung des 5G-Network-Security Domänenmodells[8]. Der Teil IV beschäftigt sich mit den abgeleiteten übergeordneten Empfehlungen zur Weiterentwicklung der Cybersicherheit bei allen Stakeholdern.

In Summe wurden in acht, jeweils ca. 6 Stunden dauernden Workshops über 500 Gefahren identifiziert, die in weiterer Folge zu 131 Einzelrisiken zusammengefasst und bewertet wurden. Diese Bewertung fand auf Basis eines in der Branche abgestimmten und jetzt aktualisierten Kriterienkatalogs statt, womit bereits eine wesentliche Leistung der Risikoanalyse hervorsticht. Die Begriffe hohes, mittleres und geringes Risiko basieren daher auf einem objektivierten und für alle TELKOs und ISPs skalierenden gemeinsamen Verständnis für Häufigkeiten von (Schad-) Ereignissen und deren Auswirkungsdimension. Zusätzlich bzw. zu Beginn der Überarbeitung der bestehenden Risikobetrachtungen wurden drei sehr intensive Workshops zur 5G Cybersecurity durchgeführt. Ergebnisse aus diesen Workshops wurden seitens des BKA als Grundlage für die Übermittlung des „national risk assessment process for 5G network infrastructures“[9] der jeweiligen Mitgliedsstaaten an die EU-Kommission und an die ENISA herangezogen. Daraus entstand dann das „EU coordinated

1 Siehe Lit.RTR-25, Digitalstrategie der Europäischen Kommission

2 Siehe Lit.RTR-26, ENISA Threat Landscape for 5G Networks

3 Siehe Lit. RTR-30, Empfehlung (EU) 2019/534 der Kommission vom 26. März 2019

4 Siehe Lit. RTR-33, Cybersecurity of 5G networks: EU Toolbox of risk mitigating measures

5 Siehe Lit.RTR-27, NIS-Fact Sheet 08/2018

6 Siehe Lit.RTR-34, Netz- und Informationssystemsicherheitsverordnung

7 Siehe Lit.RTR-35, Telekom-Netzsicherheitsverordnung 2020

8 Siehe Lit. RTR-36, 3GPP TS 33.501: Security architecture and procedures for 5G System

9 Siehe https://ec.europa.eu/commission/presscorner/detail/de/STATEMENT_19_4266

risk assessment of the cybersecurity of 5G networks“[10] und in weiterer Folge die „Cybersecurity of 5G networks EU Toolbox of risk mitigating measures“[11]. Die in diesem Prozess identifizierten Risiken wurden in den bestehenden Risikokatalog eingearbeitet. Die 131 Einzelrisiken wurden in mehreren Iterationen zu 15 Aggregationsrisiken zusammengefasst.

Alle Risiken wurden unter mehreren Gesichtspunkten 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 zu Risiken. Hier ist klar abzugrenzen, dass die Versorgungssicherheit mit Telekommunikations- und Internetdienstleistungen gegenüber den rein finanziellen Risiken für die jeweilige Organisation im Vordergrund steht.

Alle Risiken wurden in einem „Worst Case“, einem „Best Case“ und 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.

Für die Darstellung der 15 Aggregationsrisiken wurde der „Worst-Case“-Fall herangezogen. Es wurden für die Betrachtung drei hohe Risiken und 11 mittlere Risiken identifiziert.

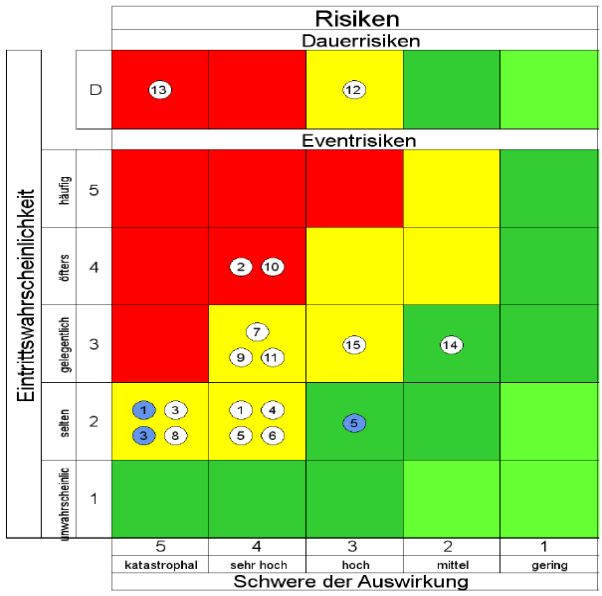


Abbildung 1: Aggregationsrisiken Übersicht

- 13, Verwundbarkeiten bei Hard- und Software
- 02, Vorsätzliche Beschädigung, Zerstörung, Diebstahl wichtiger Betriebsmittel
- 10, Vertraulichkeitsverlust von geschützten Informationen
- 12, Mängel in der Betriebsführung
- 07, Mangelhaftes Notfall-, Krisen- und Kontinuitäts-Management
- 09, Defizite bei Identity and Access Management (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
- 15, Ausfall wesentlicher Betriebsmittel, insbesondere Strom

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.

[10] Siehe Lit.RTR-32, EU coordinated risk assessment of the cybersecurity of 5G networks

[11] Siehe Lit.RTR-33, Cybersecurity of 5G networks EU Toolbox of risk mitigating measures

2 fasst de facto drei wesentliche Aspekte betrieblicher Verfügbarkeitsaspekte zusammen. Einmal ungewollte, aber 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 Nr. 10 adressiert die zunehmende Komplexität, kryptographische Methoden effektiv zu implementieren und deren Wirksamkeit über den gesamten Life-Cycle hinweg auch „nachzuweisen".
Die Einzelrisiken wurden in 12 Risikokategorien zusammengefasst. Innerhalb dieser Risikokategorien wurden 31 Empfehlungen erarbeitet, die mehreren IKT-Branchen-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 soll. Neu hinzugekommen ist eine erste Aufwandsschätzung, um den Implementierungs- und Fortschreibungsaufwand transparenter darzustellen.

Zu jedem Einzel- und Aggregationsrisiko wurden Minimierungsmaßnahmen vorgeschlagen. Viele davon sind in den meisten Unternehmen bereits umgesetzt.

Die Aggregationsrisiken wurden aus der betrieblichen Sicht in ihrer Risikohöhe bestätigt. Die Aggregationszuordnungen wurden jedoch verändert und es wurde ein zusätzliches Risiko Nr. 15 hinzugefügt. Es betrifft hier im Wesentlichen die Gefahren durch Ausfall von Betriebsmitteln. Die durch blaue Kreise in roten Dreiecken dargestellten monetären Bewertungen wurden überarbeitet.

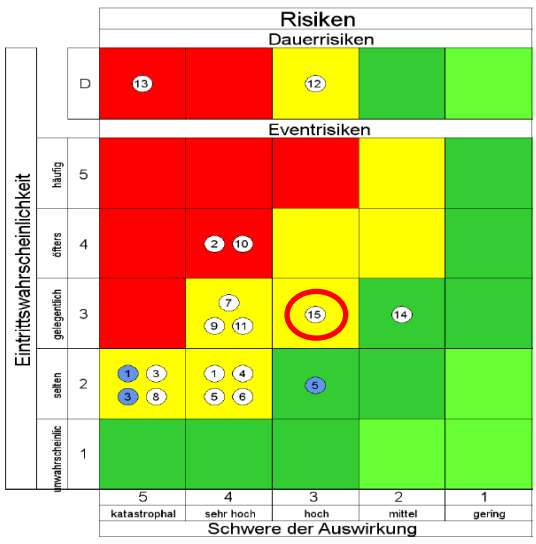


Abbildung 2: Aggregationsrisiken V3.0-2020

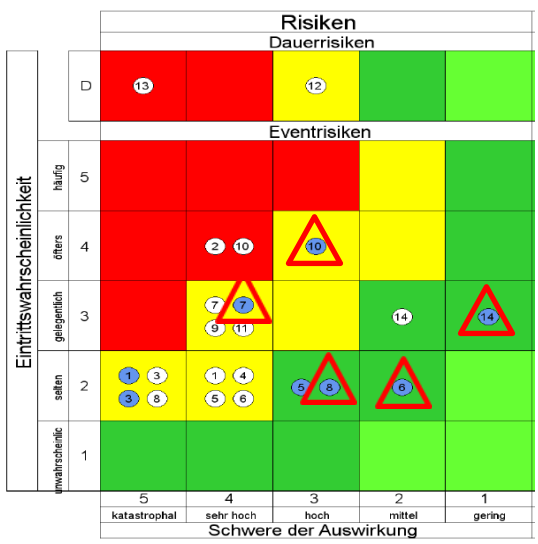


Abbildung 3: Aggregationsrisiken V2.0-2019

Die Ergebnisse wurden in einer Expertengruppe, bestehend aus Vertretern verschiedener Organisationsgrößen, der Interessensvertretung der Internetserviceprovider in Österreich sowie unter aktiver Beteiligung von BMLRT, BMI, BKA und der RTR erarbeitet. Im Jahr 2020 wurden die Mehrheit der Workshops im Rahmen von Videokonferenzen durchgeführt.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Teil I Methodik und Vorgehensweise

1. Grundsätzlicher Aufbau der Risikoanalyse

Die vorliegende Risikoanalyse ist methodisch analog zur RTR-Branchen-Risikoanalyse V1.0-2018 aufgebaut. Sie liegt in vier Teilen vor:

- Teil I beschreibt die allgemeine Herangehensweise und Methode zur Risikoidentifikation und Bewertung. Die Vorgehensweise orientiert sich an den Vorgaben der ISO 31000, „Risk management", IEC/ISO 31010, „Risk assessment techniques" und der ONR 49002-2, „Risikomanagement für Organisationen und Systeme, Teil 2: Leitfaden für die Methoden der Risikobeurteilung".
- Der Teil II, Kontexterfassung, befasst sich mit der Einbettung der Branchenrisikoanalyse in die nationalen und internationalen Programme und Vorgaben zur Cybersicherheit, u. a. der NIS[12]-Richtlinie, NISG[13], NISV und TK-NSiV 2020 auf Basis der Grundlagen des §16a Abs 9 TKG 2003 idF BGBl. I Nr. 90/2020.
- Im Teil III, Ergebnisdarstellung, werden die Anpassungen und Erweiterungen des Gefahrenkatalogs und die darauf aufbauenden Einzelrisiken dargestellt. Insbesondere werden hier die Ergebnisse der drei 5G-Security Workshops eingearbeitet. Die daraus resultierenden Einzelrisiken wurden auch im Aggregationsprozess berücksichtigt. In einem weiteren Schritt werden die Erkenntnisse aus dem ersten gemeinsamen Workshop mit der Energiewirtschaft mit Blick auf mögliche Kaskadeneffekte dargestellt.
- Aus der Zusammenschau aller Einzel- und Aggregationsrisiken wurden Maßnahmen & Empfehlungen abgeleitet, die im Teil IV aufbereitet sind.

Alle Details werden in den entsprechenden Anhängen aufbereitet.

2. Zielsetzungen der Aktualisierung der Risikoanalyse

2.1 Allgemeines

Das Verfahren der Gefahrenidentifikation und Bewertung wird als Risikomanagementprozess im Rahmen einer Public-private-Partnership (PPP) verstanden. Eine wiederkehrende Evaluierung der Ergebnisse ist daher notwendig. Die Periodizität richtet sich hier nach aktuellen Entwicklungen und wird durch den Lenkungsausschuss determiniert. Die Umsetzung erfolgt im Rahmen von Expertenworkshops. Mit Blick auf einen kontinuierlichen Verbesserungsprozess wurde eine zweijährige Periode ins Auge gefasst.
Für die vorliegenden Betrachtungen, insbesondere für die Zusammenstellung der Empfehlungen wurde ein Prognosehorizont bis 2025 vereinbart.

[12] 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

[13] Siehe Lit.RTR-03, NISG

2.2 Zielsetzungen der Aktualisierung

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

- Grundsätzliche Evaluierung der bestehenden Einzel- und Aggregationsrisiken. Eine Überprüfung der Risikobewertung wird hier als zwingend erachtet, da Maßnahmen zur Risikominimierung im Rahmen des kontinuierlichen Verbesserungsprozesses bei den Organisationen implementiert werden.
- Einarbeitung von Gefahren und die damit verbundenen Risiken durch Einführung bzw. Implementierung von neuen Technologien. Hier steht vor allem die 5G-Technologie im Vordergrund.
- Andere Branchen haben einen ähnlichen Gefahrenidentifikations- und Bewertungsprozess durchlaufen. Insbesondere die auf der Hand liegenden Interdependenzen zwischen der IKT- und der Energieversorgungsindustrie erzwingen einen intensiveren Informationsaustausch. Dieser wurde im Rahmen dieses Evaluierungsschrittes begonnen und wird fortzusetzen sein.

Nicht ausschließlich, aber sicherlich stark katalysiert durch die Ergebnisse der ersten Branchenrisikoanalyse, die verschiedenen Vorgaben aus dem TKG, die neue TK-NSiV 2020, NISG bzw. NISV wurde in den letzten Jahren intensiv an der Implementierung von Informationssicherheitsmanagementsystemen oder vergleichbaren Managementsystemen gearbeitet, um einen definierten Mindestsicherheitsstandard erreichen zu können.
Ein übergeordnetes Ziel dieses PPP-Prozesses ist es daher, Gefahren zu identifizieren, die eine **nennenswerte** Auswirkung auf die durch Telekomunikations- und Internetserviceprovider erbrachten Dienstleistungen haben können. Aus dieser übergeordneten Sicht heraus wird die Nutzung und Anwendung von Informations- und Kommunikationstechnologie(n) durch

- Natur- und Elementarereignisse,
- kriminelle und/oder terroristische Aktivitäten (intentionale Gefahren) im Cyberraum,
- technische oder, besser gesagt, technologische Entwicklungen bzw. Fehler oder Defizite
- sowie durch den Faktor Mensch maßgeblich beeinflusst.

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. Die Ergebnisse der Betrachtungen sollen für alle Organisationsgrößen vergleichbar bleiben bzw. sein. Im Rahmen der Risikobewertungen müssen Aussagen zu „Erwartungswerten" für Stör- oder Schadereignisse prognostiziert oder, besser gesagt, abgeschätzt werden. Wie bereits erwähnt, wurde der Prognosehorizont für die Erfassung und Bewertung von Risiken mit 2025 festgelegt.
In vielen Fällen, insbesondere bei der Bewertung von intentionalen Gefahren, verfügt man bis dato über wenig Erfahrung bzw. belastbare Daten, um eine objektivierte „Prognose" zu Eintrittswahrscheinlichkeiten abgeben zu können. Hier wurde der Begriff der Machbarkeit eingeführt und durch die Risikobewertungskriterien (vgl. dazu auch Abschnitt Allgemeines

zur Herleitung der Bewertungskriterien) so abgestuft, dass daraus eine einheitliche Risikomatrix zusammengestellt werden kann.

Es ist in diesem Zusammenhang wichtig darauf hinzuweisen, dass die identifizierten und bewerteten Risiken immer nur **in Relation zueinander** eine valide Aussage erlauben. Es wird nicht der Anspruch erhoben, dass die identifizierten Risiken eine *absolute* Position in der Risikomatrix einnehmen.

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

2.3 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.

3. Methodik der Risikoanalyse

Der PPP-Prozess entspricht normativen Vorgaben zum Risikomanagement[14]. Um dem PPP-Gedanken entsprechend Rechnung zu tragen, wurden seitens der Rundfunk und Telekom Regulierungs-GmbH (RTR) zwei maßgebliche Projekt- und Arbeitsgruppen eingerichtet:

- Ein Lenkungsausschuss (LSA), der die Schnittstelle zur Österreichischen Cyber Security Strategie (ÖSCS), zur Österreichischen Sicherheitsstrategie im Rahmen der Umfassenden Sicherheitsvorsorge (USV), zur Cyber Sicherheit 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) und CERT.AT.

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

3.1 Übersicht des Risikoidentifikations & Bewertungsprozesses

Der Risikoerfassungs- und -bewertungsprozess wurde gemäß Abbildung 4 durchgeführt.

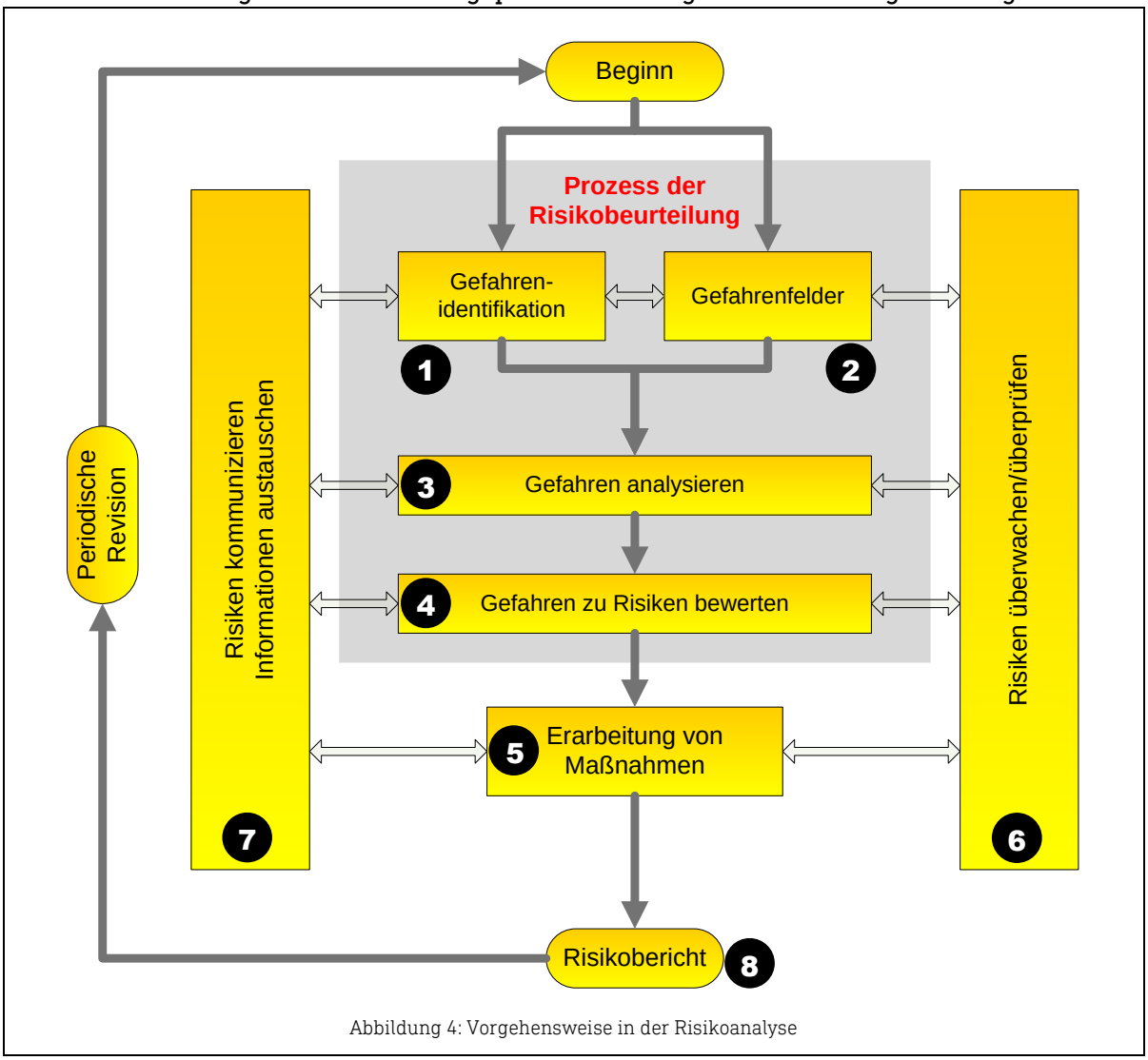


Abbildung 4: Vorgehensweise in der Risikoanalyse

3.1.1 PROZESSSCHRITT 1, GEFAHRENIDENTIFIKATION

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

- 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 on Threats and Assets - V1.2, August 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-Grundschutz-Kompendium (BSI-IT-GS)
- ENISA 5G Threat Landscape (5G TL)
- NIS CG Cybersecurity of 5G networks: EU Toolbox of risk mitigating measures (5G EU Toolbox)

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 526 Einzelgefahren zusammengestellt und in weiterer Folge analysiert.

3.1.4 PROZESSSCHRITT 4, BEWERTUNG VON RISIKEN

Das Risiko wird als Produkt von Eintrittswahrscheinlichkeit und 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 526 identifizierten Gefahren zu 131 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 Case“.
- Phase III, Aggregation der 131 Einzelrisiken zu 15 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 20.10.2020 zusammen.

3.1.8 PROZESSSCHRITT 8, PERIODISCHE REVISION

Die Risikoänderungen sind durch Umsetzung von Maßnahmen entsprechend zu erfassen, um den kontinuierlichen Verbesserungsprozess (KVP) zu dokumentieren. An dieser Stelle sei darauf hingewiesen, dass eine Risikoanalyse lediglich eine Teilaufgabe eines kontinuierlichen Verbesserungsprozesses darstellt.

Teil II Kontexterfassung

4. Nationale Rahmenbedingungen

4.1 Die Österreichische Sicherheitsstrategie

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

4.2 ÖSCS

Im Rahmen der „Österreichischen Strategie für Cyber Sicherheit" (ÖSCS) wurden Strukturen geschaffen, um auf nationaler Ebene Angelegenheiten der Cybersicherheit zu behandeln: die interministerielle „Cyber Sicherheit Steuerungsgruppe", eine Struktur zur Koordination auf der operativen Ebene und, als Public-private-Partnership, die „Cyber Sicherheit Plattform", die dem Dialog zwischen Stakeholdern aus öffentlicher Verwaltung, Wirtschaft und Wissenschaft dient. Die ÖSCS sieht auch die Durchführung sektorspezifischer Risikoanalysen vor.

4.3 APCIP, Österreichisches Programm zum Schutz Kritischer Infrastrukturen

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

4.4 Umsetzung der NISG und NISV

Die Vorgaben der Richtlinie des Europäischen Parlaments und des Rates vom 06.07.2016 über Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und

Informationssicherheit in der Union, kurz NIS-Richtlinie, wurden in Österreich durch das Bundesgesetz zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystemsicherheitsgesetz – NISG, BGBl. I Nr. 111/2018) und die unmittelbar zugeordnete Verordnung NISV (BGBl. II Nr. 215/2019) umgesetzt. Hier wird auch der Kontext zum TKG geregelt. Im Wesentlichen betrifft die Telekommunikationsbranche jedoch § 10 NISV betreffend „Sektor Digitale Infrastruktur".
Mit dem Inkrafttreten des NISG bzw. der NISV werden hier auch Mindestsicherheitsstandards definiert und in weiterer Folge durch „Qualifizierte Stellen" auditiert.
Unternehmen, die öffentliche Kommunikationsnetze oder öffentlich zugängliche elektronische Kommunikationsdienste im Sinne der Richtlinie 2002/21/EG des Europäischen Parlaments und des Rates (Rahmen-Richtlinie) bereitstellen und die den besonderen Sicherheits- und Integritätsanforderungen jener Richtlinie unterliegen, unterliegen diesbezüglich weiterhin den Regelungen des Telekommunikationsgesetzes.
Das mit dem NISG eingeführte Melderegime zu Sicherheitsmaßnahmen ist mit §§ 5 und 6 TK-NSiV 2020 iVm § 16a Abs. 3 TKG 2003 bzw. Meldungen über Sicherheitsvorfälle gemäß § 16a Abs. 5 TKG 2003 harmonisiert oder klar abgegrenzt.

4.5 TK–NSiV 2020

Die im Hinblick auf die für Ende 2019 angekündigte 5G EU Toolbox unterbrochenen Arbeiten der RTR-GmbH an einer Telekom-Netzsicherheitsverordnung wurden nach Publikation der Toolbox durch die NIS Cooperation Group im Jänner 2020 fortgesetzt. Das Expertengremium der Branchenrisikoanalyse hat die Toolbox und ihre Einzelmaßnahmen sowie verschiedene Aspekte einer möglichen nationalen Umsetzung im weiteren Verlauf erörtert und den Entwurf der Verordnung ausführlich diskutiert. Nach einer öffentlichen Konsultation des Verordnungsentwurfs im Mai/Juni 2020 trat die Telekom-Netzsicherheitsverordnung 2020 („TK-NSiV 2020") schließlich am 4.07.2020 in Kraft. Neben einer Festschreibung der schon bisher aufgrund entsprechender technischer Leitlinien der ENISA geübten Branchenpraxis in Bezug auf Mindestsicherheitsmaßnahmen beim Betrieb elektronischer Kommunikationsnetze und –dienste sowie Meldepflichten bei Sicherheitsvorfällen mit beträchtlichen Auswirkungen auf Netzbetrieb bzw. Dienstebereitstellung sieht die Verordnung in Anlehnung an das NISG auch die Möglichkeit freiwilliger Meldungen bei Nichterreichen der Schwellwerte vor. Zudem stellt die Verordnung spezifische Anforderungen an Betreiber von 5G-Netzen mit insgesamt mehr als 100.000 Teilnehmern in allen von ihnen betriebenen Netzen auf und setzt damit einige der Vorgaben aus der 5G EU Toolbox um. Hervorzuheben sind in diesem Zusammenhang einerseits die Erfüllung bestimmter Standards (ISO 27001 iVm bestimmten Anforderungen aus ISO 27002/27011 sowie relevanter 3GPP-Standards und ENISA-Dokumente) und andererseits die Erfüllung mehrerer gesondert ausdrücklich angeführter Sicherheitsmaßnahmen aus der Toolbox (z.B. Betrieb von NOC/SOC in eigenen Räumen, Schutz des Managementverkehrs, physischer Schutz kritischer Netzwerkkomponenten, Multi-Vendor-Strategie etc.). Die von der Verordnung betroffenen Betreiber von 5G-Netzen haben im Hinblick auf mögliche Risikolieferanten zudem halbjährlich eine Liste von Herstellern für bestimmte nach Funktionen gegliederte Netzkomponenten zu übermitteln.

5. EU Vorgaben & ENISA

Im Rahmen der Arbeiten zur Aktualisierung der RTR-IKT-Branchenrisikoanalyse wurden durch die Expertengruppe erhebliche Ressourcen der Erfüllung der Vorgaben der

„Commission Recommendation (EU) 2019/534 of 26 March 2019 on the Cybersecurity of 5G networks“ gewidmet. Die Ergebnisse dieser Arbeit wurden unmittelbar dem geforderten „national risk assessment“ zur Verfügung gestellt und auch als Ergänzung und Update zur bestehenden IKT-Risikoanalyse eingearbeitet. Im Wesentlichen wurden hier drei Aspekte abgearbeitet:

- Einarbeitung der Vorgaben der ENISA Threat Landscape for 5G Networks
- Einarbeitung der Vorgaben der Cybersecurity of 5G networks EU Toolbox of risk mitigating measures
- Übermittlung der “findings” entsprechend den „Guidelines on common elements for 5G cybersecurity risk assessments and structured template for reporting on findings”

5.1 ENISA Threat Landscape for 5G Networks

Der Bericht „ENISA Threat Landscape for 5G Networks“ (ENISA-Bedrohungslandschaft für 5G-Netze) liefert einige der relevantesten Aspekte im Zusammenhang mit der Art, dem Ursprung und den Zielen von Cybersicherheitsbedrohungen, die auf diese neue Generation mobiler Netze abzielen. Dieser Bericht stellt einen ersten Versuch dar, die kritischsten Komponenten in einem 5G-Netz zu identifizieren, die zum Ziel verschiedener Bedrohungen aus dem Cyberraum werden können. Die Erstellung einer umfassenden 5G-Architektur, die alle wesentlichen Elemente/Funktionen abdeckt, stellt eine extrem anspruchsvolle Aufgabe dar. Die Schaffung einer kohärenten und umfassenden Architektur, die Elemente aus bestehenden generischen 5G-Architekturen verwendet, erfordert eine Abstimmung mit bestehenden und laufenden Arbeiten, die von Standardisierungsgremien und anderen relevanten Einrichtungen (z.B. 3GPP, 5G PPP, ITU, ETSI und GSMA) durchgeführt werden. Die umfassende 5G-Architektur, die in diesem Bericht vorgestellt wird, wird in verschiedenen "Domänen" näher erläutert, die weitere Informationen zu den sensibelsten 5G-Komponenten enthalten.
Mögliche IKT-Gefahren von und aus diesen Domänen heraus wurden im Rahmen der IKT-Branchen Risikoanalyse detailliert analysiert.

5.2 Cybersecurity of 5G networks EU Toolbox of risk mitigating measures

Die Ziele dieser Toolbox bestehen darin, einen möglichen gemeinsamen Satz von Maßnahmen zu identifizieren, die in der Lage sind, die wichtigsten Cybersicherheitsrisiken von 5G-Netzen, wie sie in dem von der EU koordinierten Risikobewertungsbericht identifiziert wurden, abzuschwächen und eine Anleitung für die Auswahl von Risikominimierungsverfahren zu geben, die in nationalen Programmen berücksichtigt werden können bzw. sollen.
Die von der EU koordinierte Risikobewertung identifiziert eine Reihe von Risikokategorien von strategischer Bedeutung aus einer EU-Perspektive, die durch konkrete Risikoszenarien veranschaulicht werden. Diese widerspiegeln relevante Kombinationen von Verwundbarkeiten, Bedrohungen und Bedrohungsakteuren sowie die identifizierten Mittel.
Im Rahmen der Identifikation von Risiken in 5G-Netzen wurden auch die Vorgaben der „Cybersecurity of 5G networks: EU Toolbox of risk mitigating measures“ mit in den Risikokatalog eingearbeitet, vergleiche dazu auch Aufbau der Risikoerfassung, Spalte N.

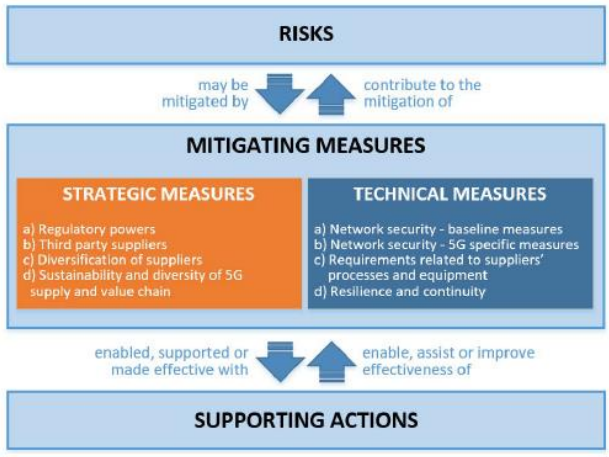


Abbildung 5: Aufbau und Inhalt der 5G EU Toolbox

Die Inhalte der Toolbox sind in nebenstehender Abbildung zusammengefasst.
Im Rahmen der Diskussionen wurden insbesondere die Strategic Measures [SM], Technical Measures [TM] und Supporting Actions [SA] beleuchtet. Sowohl die Strategic als auch die Technical Measures werden in der Telekom-Netzsicherheitsverordnung 2020 umgesetzt bzw. berücksichtigt.

Folgende „Risk-mitigating measures" wurden seitens der 5G EU Toolbox definiert.

5.2.1 STRATEGIC MEASURES

- SM01 Strengthening the role of national authorities;
- SM02 Performing audits on operators and requiring information;
- SM03 Assessing the risk profile of suppliers and applying restrictions for suppliers considered to be high risk - including necessary exclusions to effectively mitigate risks- for key assets;
- SM04 Controlling the use of Managed Service Providers (MSPs) and equipment suppliers' third line support;
- SM05 Ensuring the diversity of suppliers for individual MNOs through appropriate multi-vendor strategies;
- SM06 Strengthening the resilience at national level;
- SM07 Identifying key assets and fostering a diverse and sustainable 5G ecosystem in the EU;
- SM08 Maintaining and building diversity and EU capacities in future network technologies.

5.2.2 TECHNICAL MEASURES

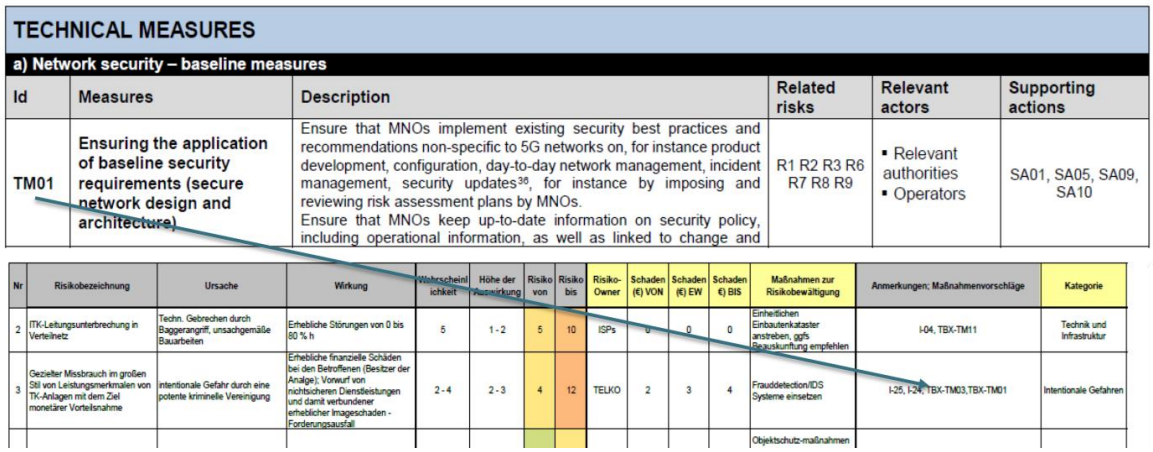
- TM01 Ensuring the application of baseline security requirements (secure network design and architecture);
- TM02 Ensuring and evaluating the implementation of security measures in existing 5G standards;
- TM03 Ensuring strict access controls;
- TM04 Increasing the security of virtualised network functions;
- TM05 Ensuring secure 5G network management, operation and monitoring;

- TM06 Reinforcing physical security;
- TM07 Reinforcing software integrity, update and patch management;
- TM08 Raising the security standards in suppliers' processes through robust procurement conditions;
- TM09 Using EU certification for 5G network components, customer equipment and/or suppliers' processes;
- TM10 Using EU certification for other non 5G-specific ICT products and services (connected devices, cloud services);
- TM11 Reinforcing resilience and continuity plans.

5.2.3 SUPPORTING ACTIVITIES

- SA01 Reviewing or developing guidelines and best practices on network security;
- SA02 Reinforcing testing and auditing capabilities at national and EU level;
- SA03 Supporting and shaping 5G standardisation;
- SA04 Developing guidance on the implementation of security measures in existing 5G standards;
- SA05 Ensuring the application of standard technical and organisational security measures through specific EU-wide certification scheme;
- SA06 Exchanging best practices on the implementation of strategic measures, in particular national frameworks for assessing the risk profile of suppliers;
- SA07 Improving coordination in incident response and crisis management;
- SA08 Conducting audits of interdependencies between 5G networks and other critical services;
- SA09 Enhancing cooperation, coordination and information sharing mechanisms;
- SA10 Ensuring 5G deployment projects supported with public funding take into account cybersecurity risks

5.2.4 DARSTELLUNG DER ZUORDNUNG ZU DEN RISIKEN



TECHNICAL MEASURES

a) Network security – baseline measures

Id	Measures	Description	Related risks	Relevant actors	Supporting actions
TM01	**Ensuring the application of baseline security requirements (secure network design and architecture)**	Ensure that MNOs implement existing security best practices and recommendations non-specific to 5G networks on, for instance product development, configuration, day-to-day network management, incident management, security updates[36], for instance by imposing and reviewing risk assessment plans by MNOs. Ensure that MNOs keep up-to-date information on security policy, including operational information, as well as linked to change and	R1 R2 R3 R6 R7 R8 R9	▪ Relevant authorities ▪ Operators	SA01, SA05, SA09, SA10

Nr	Risikobezeichnung	Ursache	Wirkung	Wahrscheinlichkeit	Höhe der Auswirkung	Risiko von	Risiko bis	Risiko-Owner	Schaden (€) VON	Schaden (€) EW	Schaden € BIS	Maßnahmen zur Risikobewältigung	Anmerkungen; Maßnahmenvorschläge	Kategorie
2	ITK-Leitungsunterbrechung in Verteilnetz	Techn. Gebrechen durch Baggerangriff, unsachgemäße Bauarbeiten	Erhebliche Störungen von 0 bis 80 % h	5	1 - 2	5	10	ISPs	0	0	0	Einheitlichen Einbautenkataster anstreben, ggfs Bauauskunftung empfehlen	I-04, TBX-TM11	Technik und Infrastruktur
3	Gezielter Missbrauch im großen Stil von Leistungsmerkmalen von TK-Anlagen mit dem Ziel monetärer Vorteilsnahme	intentionale Gefahr durch eine potente kriminelle Vereinigung	Erhebliche finanzielle Schäden bei den Betroffenen (Besitzer der Anlage); Vorwurf von nichtsicheren Dienstleistungen und damit verbundener erheblicher Imageschaden - Forderungsausfall	2 - 4	2 - 3	4	12	TELKO	2	3	4	Frauddetection/IDS Systeme einsetzen	I-25, I-24, TBX-TM03,TBX-TM01	Intentionale Gefahren
												Objektschutz-maßnahmen		

Abbildung 6: Berücksichtigung der 5G EU Toolbox Measures

5.3 Radio Equipment Directive

Die Experten der Branchenrisikoanalyse haben auch die Bitte des BMLRT zur Unterstützung bei der Befüllung des „gezielten Konsultationsfragebogen zu Rekonfigurierbaren Funksystemen (Reconfigurable Radio Systems, RRS)“ bearbeitet. Die Europäische Kommission untersucht derzeit die potenziellen Auswirkungen von alternativen Wegen, um sicherzustellen, dass rekonfigurierbare Funksysteme, die in den Binnenmarkt in Verkehr gebracht werden, weiterhin mit der RED, Radio Equpiment Directive, kompatibel bleiben. Dies soll auch nach der Installation neuer oder geänderter Software gewährleistet werden. Im Kontext zur 5G-Technologie wurden hier Schnittstellen zur RED identifiziert. In einem engen Diskurs mit der Expertengruppe wurden hier mögliche zusätzliche Risiken identifiziert. Im Ergebnis wurden keine zusätzlichen Gefahren erkannt. Man hat auch die Schnittstelle hin zur RED klarer definiert. Die in der RED definierten Securityanforderungen behandeln zwar auch das vorgelagerte IKT-Netz. Im Wesentlichen wird aber primär rein die Funkschnittstelle durch die RED erfasst.

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. In Summe wurden in 11 jeweils ca. 6 Stunden dauernden Workshops 526 Gefahren identifiziert:

- Dazu wurde in einem ersten Schritt der bestehende Gefahrenkatalog (siehe Abbildung 7: Struktur der allgemeinen IKT Gefahrenlandschaft) evaluiert.
- In drei Workshops zur 5G Cybersecurity wurde das 5G Domänenmodell (siehe Abbildung 8: 5G-spezifisches Gefahrenmodell) in einen Gefahrenkatalog umgearbeitet.

Es stehen also derzeit zwei Gefahrenkataloge zur Verfügung:

- Gefahrenkatalog I – Allgemeine IKT-Gefahren
- Gefahrenkatalog II- 5G-spezifische Gefahren

6.1.1 ALLGEMEINES IKT-GEFAHRENMODELL

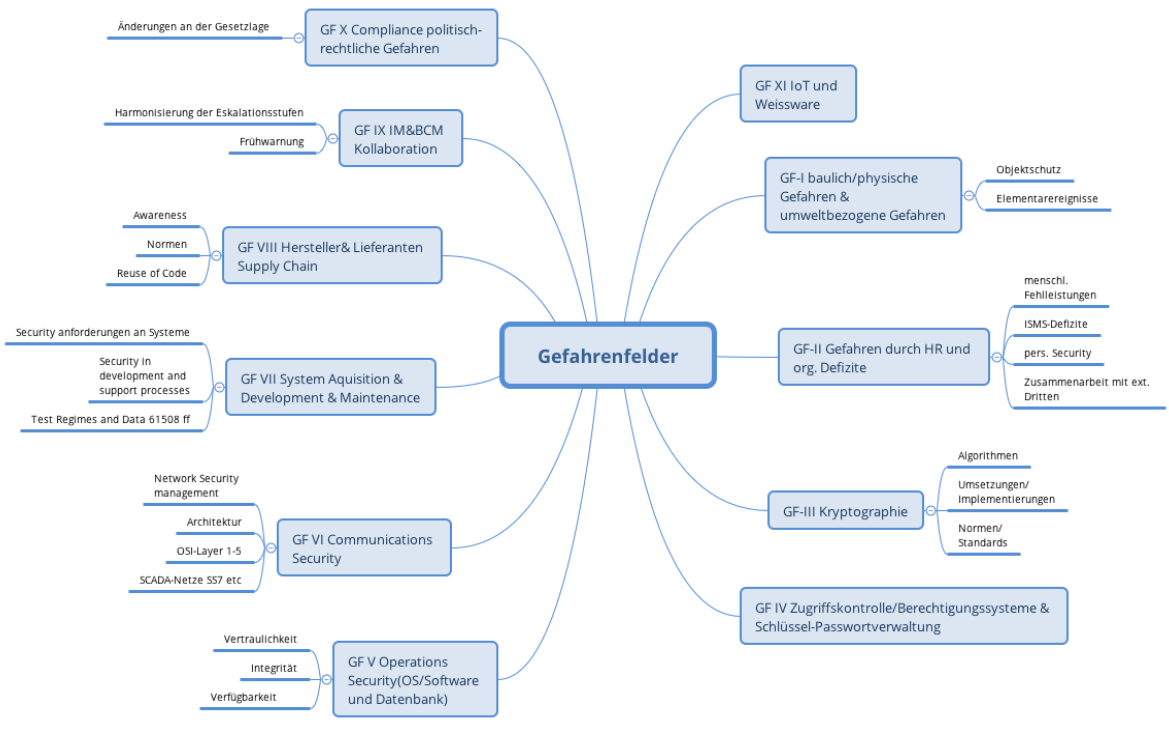


Abbildung 7: Struktur der allgemeinen IKT Gefahrenlandschaft

6.1.2 5G-SPEZIFISCHES GEFAHRENMODELL

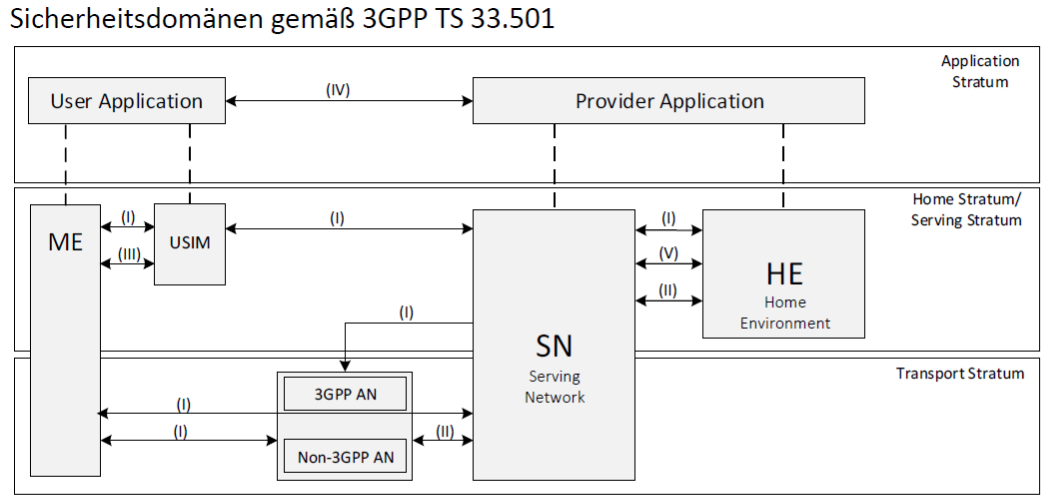


Abbildung 8: 5G-spezifisches Gefahrenmodell[15]

6.2 Kurzbeschreibung der allgemeinen 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.

[15] Siehe Lit.RTR-36, 3GPP TS 33.501: Security architecture and procedures for 5G System

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 werden 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 Kurzbeschreibung der 5G-spezifischen Gefahrenfelder

Der Gefahrenidentifikation gliedert sich hier nach 6 „Sicherheitsdomänen“, gemäß 3GPP TS 33.501[16].

6.3.1 ZUGANGSNETZ (NETWORK ACCESS SECURITY)

Darunter werden aus Sicht der 5G-eigenen Architektur die Gefahren subsumiert, die von und bei den „Zugangsnetzpunkten“ möglich/denkbar sind. (Defizite an der Luftschnittstelle, unsichere Abläufe zwischen User Equipment und Kernnetz etc.)

6.3.2 NETZWERKDOMÄNE (NETWORK DOMAIN SECURITY)

Hier wird die Sicherheitsarchitektur des Netzwerks angesprochen. In diesem Kontext wurden die im Standard definierten „mandatory features“ und optionalen Features diskutiert. Hier besteht die Gefahr, dass beispielsweise mandatory features nicht richtig oder gar nicht implementiert werden.

6.3.3 NUTZERDOMÄNE (USER DOMAIN SECURITY)

Hierunter werden de facto alle Gefahren der „Malversation“ von Software durch Nutzer an der Schnittstelle zum Endgerät verstanden.

6.3.4 APPLIKATIONSDOMÄNE (APPLICATION DOMAIN SECURITY)

Obwohl diese Domäne vom o. a. Standard explizit ausgenommen wurde, hat man sich im Rahmen der Gefahrenidentifikationsworkshops mit Szenarien bzw. Gefahren, wie zum Beispiel der Möglichkeit/Gefahr, dass Applikationen sich alleine auf die Sicherheitsfunktionen der Zugangstechnologien verlassen, beschäftigt.

[16] Siehe Lit.RTR-36, 3GPP TS 33.501: Security architecture and procedures for 5G System

6.3.5 SBA-DOMÄNE (SERVICE BASED ARCHITECTURE DOMAIN SECURITY)

Gefahren, die sich hier ergeben, wurden in einen allgemeinen Teil verschoben.

6.3.6 SICHTBARKEIT UND KONFIGURIERBARKEIT (VISIBILITY AND CONFIGURABILITY)

Hier wurden Gefahren erfasst, die sich im Wesentlichen mit versehentlicher und nicht erkannter Nutzung unsicherer Dienste beschäftigen. Darunter wird u. a. keine durchgängig gleich sichere / Absicherung von Kommunikation verstanden, bedingt durch unterschiedliche Behandlung von Basisfunktionen bei unterschiedlichen Zugangstechnologien (WLAN, 5G-Acces-Points etc.)

6.4 Aufbau der Gefahrenkataloge

6.4.1 ALLGEMEINER IKT GEFAHRENKATALOG

Der allgemeine 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-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 allgemeinen IKT Gefahrenkatalogs

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

6.4.2 5G SPEZIFISCHER GEFAHRENKATALOG

Der Gefahrenkatalog ist wie folgt aufgebaut:

- Domänen Nummer,
- Bezeichnung der Domäne
- und die in den jeweiligen Domänen adressierten Gefahren

Nr.	5G-Domänenmodell gem. 3GPP TS 33.501 V15.4.0 (2019-03)	Gefahrenliste 4G/5G
	Bezeichnung der Domäne	**Gefahrenbezeichnung / Beschreibung**
I	**Network access security**	Defizite im Certificate handling/TLS Handling (revoking, fehlende Möglichkeit, die CAs rasch zu widerrufen) (Identitätsdiebstahl), Netzkomponenten und/oder Netzelemente erlauben gefälschte Identitätiten
		Gefahr von Downgradeattacken
		Gefahr von Fehlkonfigurationen durch die Komplexität
		Gefahr des Trackings von Nutzern durch Dritte, Nichteinführung der Verschlüsselung auf der Funkschnittstelle und damit weiter Tracking möglich
		Gefahr, dass zu wenige Verschlüsselungsalgorithmen im Standard verfügbar und verpflichtend sind
		Gefahr von unsicheren Abläufen zwischen UE (User Equipment) und Kernnetz
		Gefahr von Defiziten bei Network Domain Control Plane protection
		Gefahr von Defiziten in Backhaul link user plane protection
		Management plane protection over the S1 interface
III	**User domain security**	fehlende Möglichkeit der zeitnahen Information von UE-Fehlfunktionen
		Beratungsresistenz von Endnutzern
		Software Malversation User to Access Domain
IV	**Application domain security**	Gefahr von nichtkonformer /mangelnder Implementierung/State of the Art Implementierung
		fehlende Prüfung der Authentizität von Software
		Gefahr, dass Anwendungen sich auf die Sicherheitsfunktionen der Zugangstechnologien verlassen

Tabelle 2: 5G-spezifischer Gefahrenkatalog

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 im Rahmen der ersten Risikobetrachtung in mehreren Schritten erarbeitet. Während der Evaluation wurden die Beschreibungen präzisiert. 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. 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 eine Bewertungsmetrik festgelegt, die sowohl für ganz kleine Organisationen anwendbar ist als auch bei den großen bis sehr großen TELKOs und ISPs sinnvoll eingesetzt werden kann.

7.2 Festlegung der Eintrittswahrscheinlichkeiten und Machbarkeit

7.2.1 TECHNISCHE GEBRECHEN UND NATURGEFAHREN

Technische Gefahren- und Naturgefahren				Bewertung Punkte
Eintritts-wahrscheinlichkeit	Verbale Beschreibung	Mind. Häufigkeit 1mal pro		
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 3: 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 (Angriffs-methoden/Vektoren) sind bis dato unbekannt.	Wochen - Monate der Vorbereitung / Experten-niveau vgl. auch State Actors inkl. gezielter Aufklärung	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 z. B. APTs - auch in Kombination mit social Engineering	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 mitbekannten Hilfsmitteln überwunden werden müssen. (keine Automatisation der Angriffe/Vektoren)	Tage der Vorbereitung-Fachkenntnisse werden vorausgesetzt. Auch kriminelle Handlungen	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. Manipulationen durch Insider	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. Hacktivisten	5
	Aufwand wird auch immer finanziell verstanden		

Tabelle 4: 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	Genutzte 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 sind kurzzeitig ausgefallen oder verhalten sich kurzfristig fehlerhaft. Fehler sind nicht genau reproduzierbar. 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 abgegriffen und Teile davon werden veröffentlicht. Die Tat wird Einzeltätern zugeschrieben. Wiederherstellung der Vertraulichkeit mit nennenswertem Aufwand. Imageschaden.	Netze/Services/Applikationen sind dauerhaft ausgefallen und dauerhaft fehlerhaft. Wiederherstellungsaufwand hoch (ein einfacher Restart reicht nicht aus). 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 Netzen/Services/Applikationen	(wie hoch aber zusätzlich) Daten wurden im erheblichen Umfang veröffentlicht. Es kann für einzelne Personen zur Gefährdung der persönlichen Sicherheit führen. Wiederherstellung der Vertraulichkeit erheblich. Sehr hoher Imageschaden.	Netze/Services/Applikationen/Konfigurationen müssen aufgrund der Ereignisse überarbeitet werden. Wiederherstellungsaufwand sehr hoch. Eingesetzte Sicherungs-Technik muss angepasst werden. Keine grundsätzliche Änderung von Architekturen 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 einen längeren Zeitraum unbemerkt exfiltriert. Die persönliche Sicherheit von vielen Personen ist gefährdet. Wiederherstellung der Vertraulichkeit erheblich. Katastrophaler Imageschaden.	Netze/Services/Applikationen müssen aufgrund der Ereignisse komplett redesigned 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/normative 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/Organisation 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 5: Bewertung der Schadensdimension

7.4 Risikobewertungsprozess – Übersicht

Die in der Version 2.0-2019 identifizierten 135 Einzelrisiken wurden in einem ersten Schritt evaluiert. In Summen wurde 526 Gefahren in mehreren Workshops zu 131 Risiken zusammengestellt. Im Rahmen der Diskussion um die 5G-Security wurden zwei maßgebliche Schritte mit Blick auf die Risikoerhebung vollzogen.

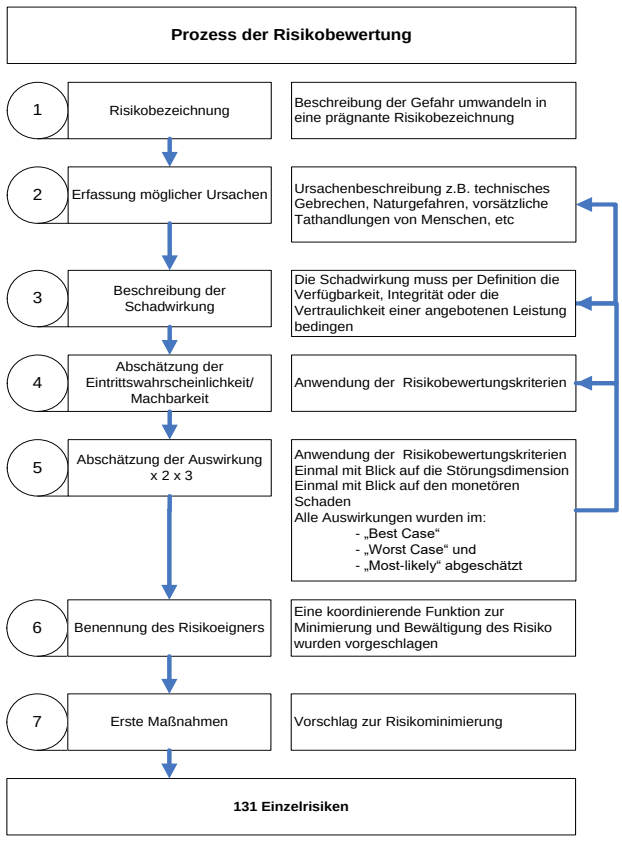


Abbildung 9: Risikobewertungsprozess

Das Ergebnis der Zusammenstellung denkbarer Gefahren im 5G-spezifischen Gefahrenkatalog dient als Grundlage der Evaluierung bzw. Ergänzung von Risiken in die bestehende Risikomatrix gemäß neben-stehendem Prozess.

Analyse der ENISA 5G Threat Landscape[17]: Dieser Arbeitsschritt wurde zweigeteilt. Die darin dargestellten Bedrohungen wurden in eine umfassende Gefahrentabelle extrahiert und den entsprechenden Domänen, der Systematik der ENISA folgend, zugeordnet.

7.5 Einarbeitung der ENISA 5G Threats in den bestehenden Einzelrisikokatalog

Die von der ENISA dargestellte Systematik zur Erfassung und Bewertung von Risiken im 5G-Kommunikationsnetzwerk ist nicht kongruent zur bereits gewählten Systematik der vorliegenden IKT-Branchen-Risikoanalyse. Es war jedoch möglich, alle Aspekte in die bestehende Risikobetrachtung einzuarbeiten. Dies wurde durch eine Zuordnung der bereits evaluierten Einzelrisiken zu den „Threats“, dargestellt in der ENISA 5G Threat Landscape Systematik, möglich. Dort, wo notwendig, wurden Einzelrisiken ergänzt bzw. entsprechend umformuliert und neu bewertet.

[17] Siehe Lit.RTR-26, ENISA THREAT LANDSCAPE FOR 5G NETWORKS

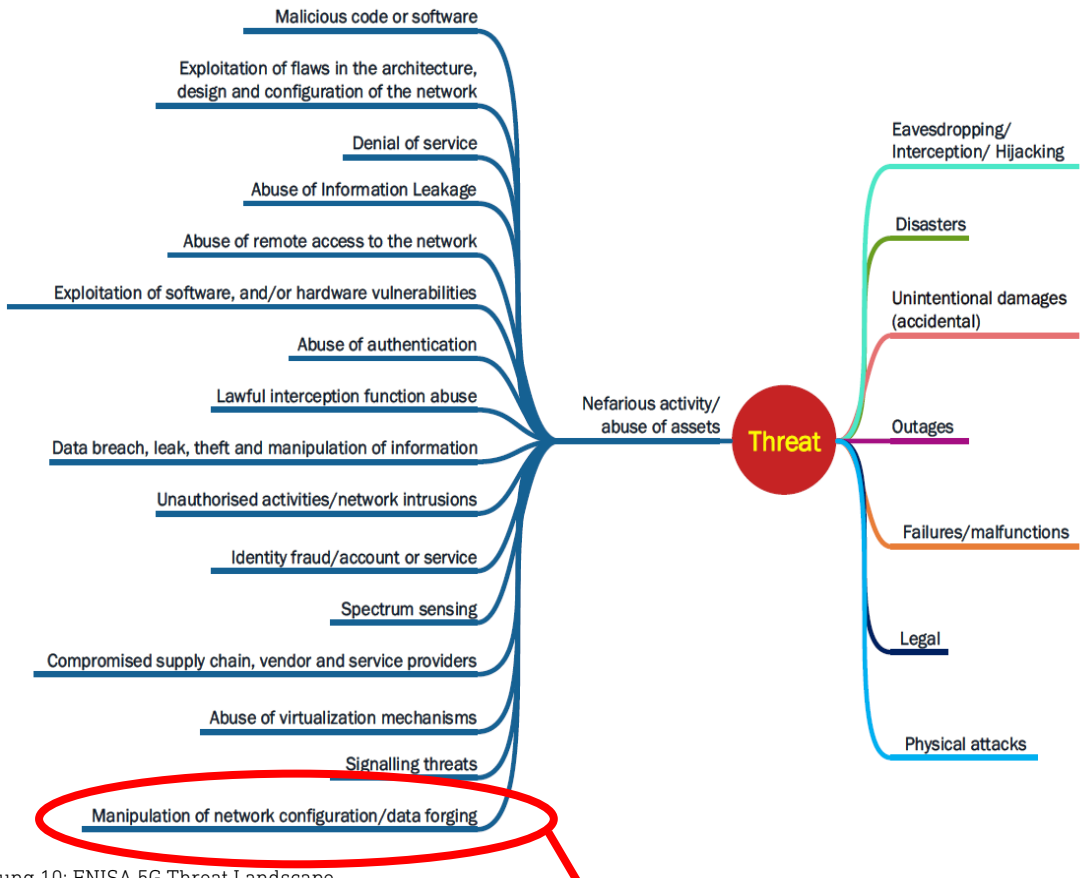


Abbildung 10: ENISA 5G Threat Landscape

Threats	Zuordnung zu Branchenrisiko Nr.
Manipulation of network configuration/data forging - Routing tables manipulation - Falsification of configuration data - DNS manipulation - Manipulation of access network and radio technology configuration data - Exploitation of misconfigured or poorly configured systems/networks - Registration of malicious network functions	66,65,70,136,36,35
Exploitation of software, hardware vulnerabilities - Zero-day exploits - Abuse of edge open application programming interfaces (APIs) - Application programming interface (API) exploitation	54,91,90,53,67

8. Ergebnisdarstellung der Einzelrisiken

8.1 Aufbau der Risikoerfassung

Die Aufbereitung der Ergebnisse soll hier kurz beschrieben werden.

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

Tabelle 6: 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
ISPs	0	0	0	Einheitlichen Einbautenkataster anstreben, ggfs. Beauskunftung empfehlen, Wegeredundanz	I-04, TBX-TM11	Technik und Infrastruktur

Tabelle 7: Teil 2 der Einzelrisikoerfassungstabelle

Fortsetzung der Tabelle

P	Q	R
Gültigkeit bis	NIS-MAP	Kaskaden, gem. Risken
11.03.21	7	G, K

Tabelle 8: Teil 3 der Einzelrisikoerfassungstabelle

- Spalte A, laufende Nummer – Entwicklungsnummer, losgelöst von der Risikohöhe. **Es ist wichtig, darauf hinzuweisen, dass aufgrund der Nachvollziehbarkeit die laufenden Nummern „Lücken" aufweisen können. So wurde z. B. das Risiko Nr. 1, Sonnensturm, ersatzlos gestrichen.**
- Spalte B, Risikobezeichnung
- Spalte C, Kurzbeschreibung der möglichen Ursache
- Spalte D, Beschreibung der Auswirkung
- Spalte E, Bewertung der Eintrittswahrscheinlichkeit nach den Bewertungskriterien (hier können auch Intervalle eingetragen werden z. B. 1-2 gleichbedeutend für einmal

in 10-20 Jahren 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 risikominimierenden 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, „Einheitlichen Einbautenkataster anstreben, ggfs. Beauskunftung empfehlen, Wegeredundanz".
- Spalte N, verweist auf die Gefahrennummer nach römisch I= Gefahrenfeld I und laufender Nummer im jeweiligen Gefahrenfeld, Die Anmerkungen, die mit TBX- beginnen, referenzieren auf die 5G EU Toolbox zu den „risk mitigation measures".
- Spalte O ordnet das Risiko einer Risikokategorie zu. Hier im konkreten Fall einmal zu Naturgefahren, einmal zu der Risikokategorie Technik und Infrastruktur.
- Spalte P, definiert eine Gültigkeitsdauer dieses Risikos. Diese wird durch den festgelegten Reviewzyklus determiniert.
- Spalte Q, hier ist das Mapping auf die seitens der NISV festgelegten Kapitel in den Fact Sheets zur Festlegung von Mindestsicherheitsstandards aufgelistet.
- Spalte R, hier wurde vermerkt, ob es sich um ein mit der Energiewirtschaft „gemeinsames" Risiko handelt (G) oder ob es sich um ein Risiko mit Kaskadenpotential handelt (K).

Die Ergebnisse der Risikobewertung aller 526 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.

8.2 Auswertung der Risikoverteilung im „Worst Case“

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

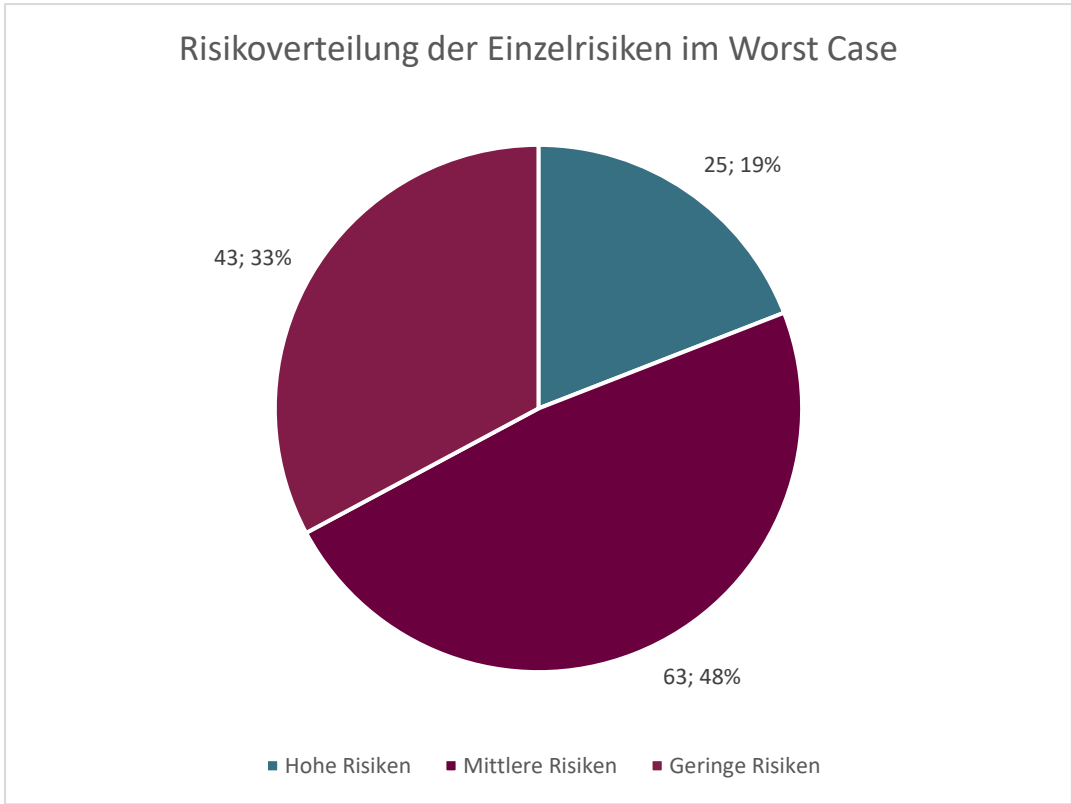


Abbildung 11: Risikoverteilung im „Worst Case“

19 % hohe Risiken, 48 % geringe Risiken und 33% mittlere Risiken stellen ein gewohntes Bild der Risikoverteilung dar.

9. Ergebnisdarstellung der Aggregationsrisiken

9.1 Aggregationsprozess

Die 131 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 nachfolgenden 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.

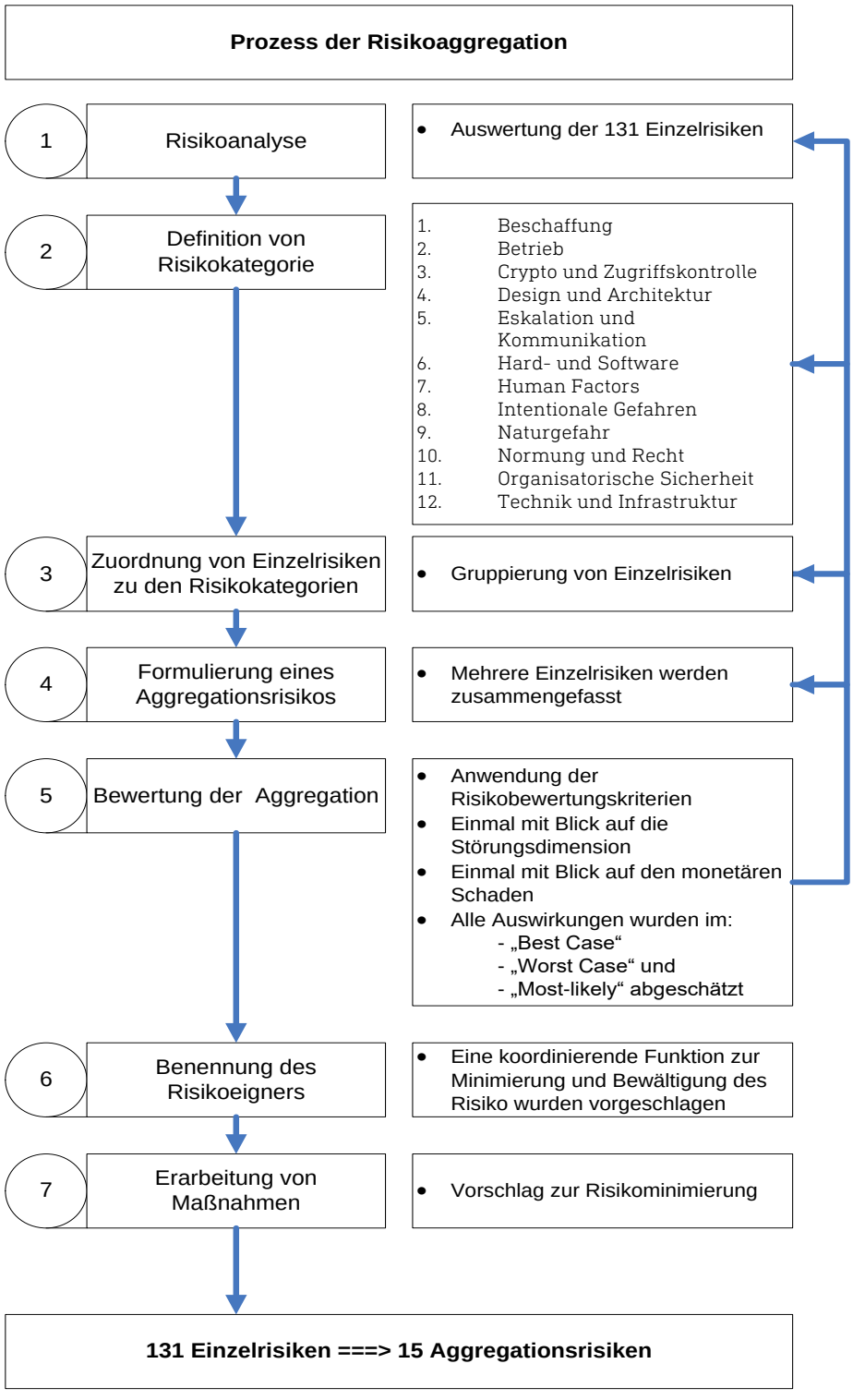


Abbildung 12: Risikoaggregationsprozess

9.2 Aggregationsrisikomatrix im „Worst Case“

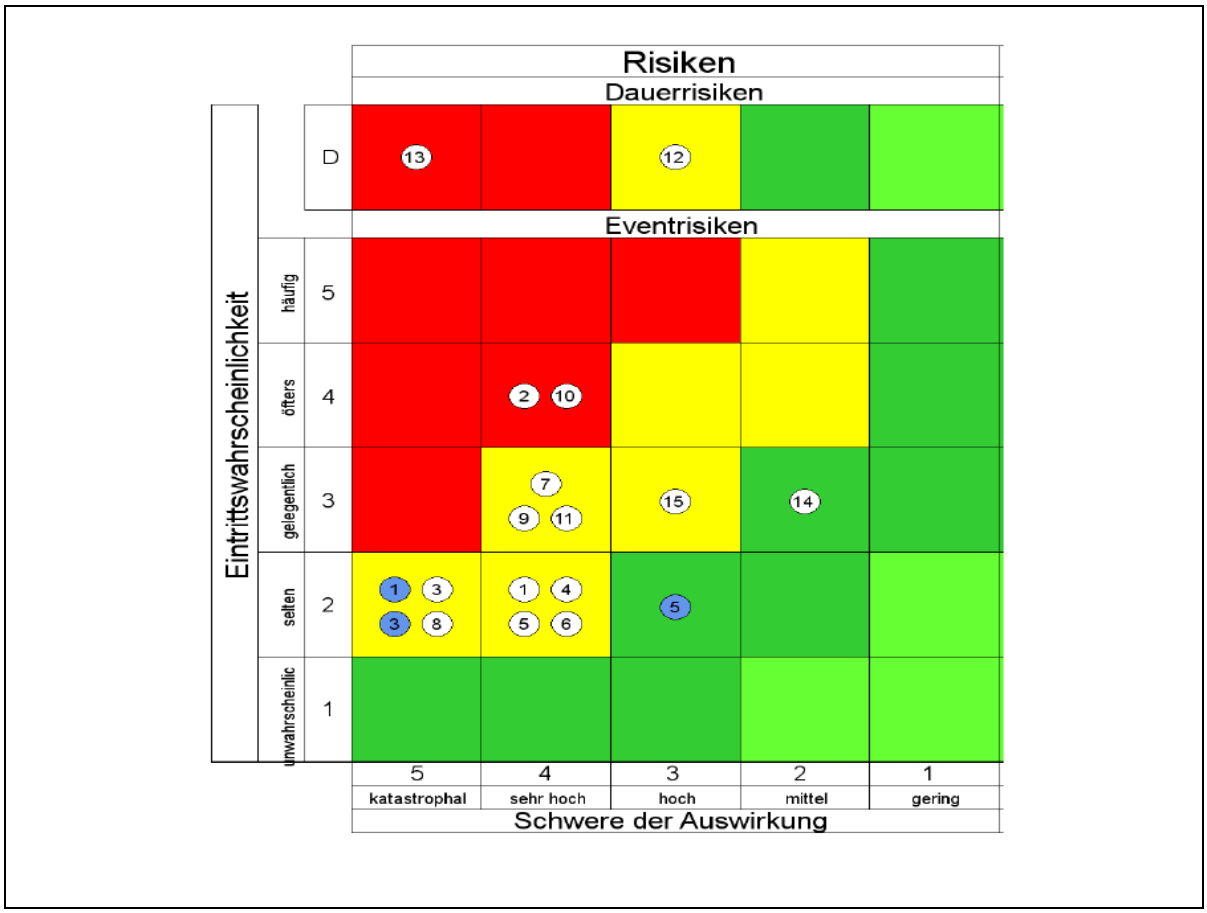


Abbildung 13: Aggregationsmatrix im "Worst Case"

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“

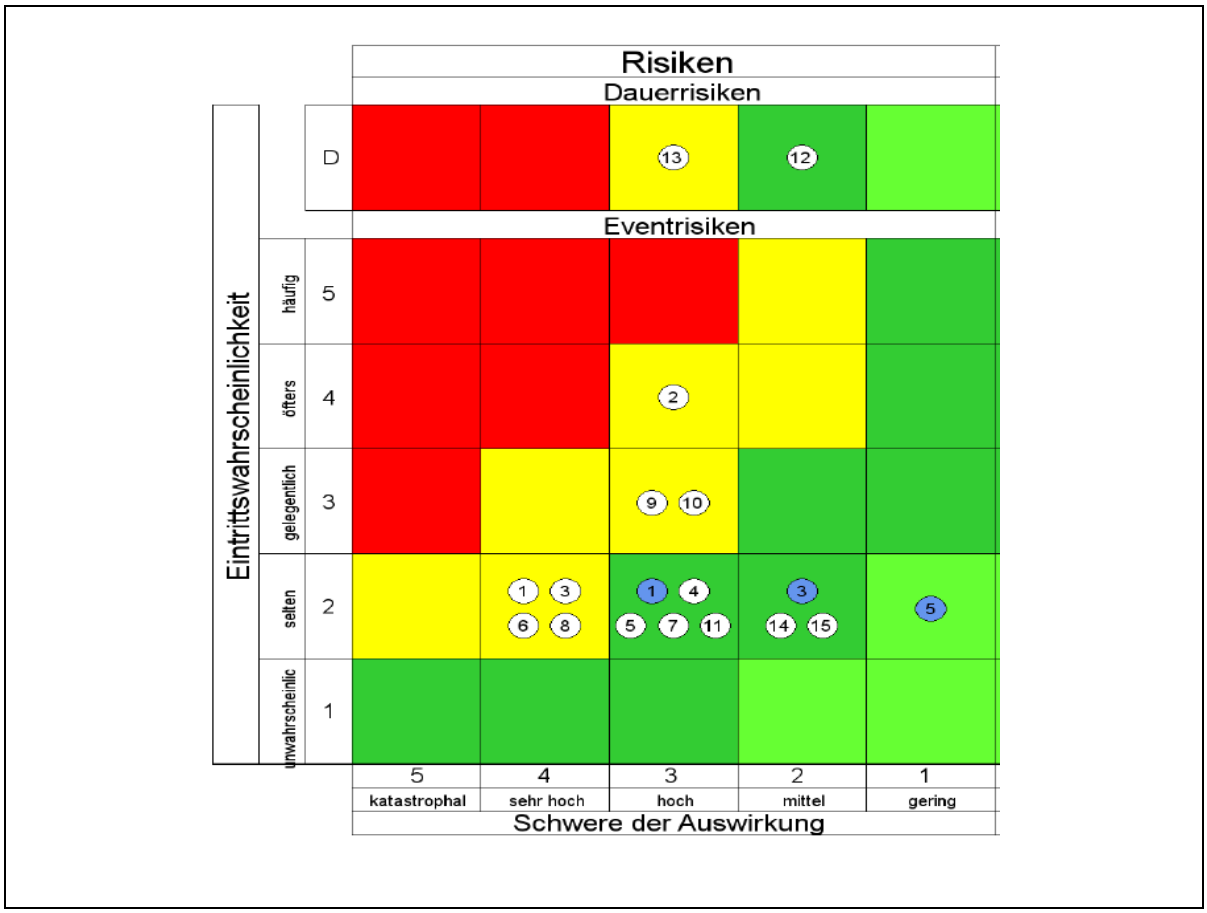


Abbildung 14: Aggregationsmatrix im "Most-likely"

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“

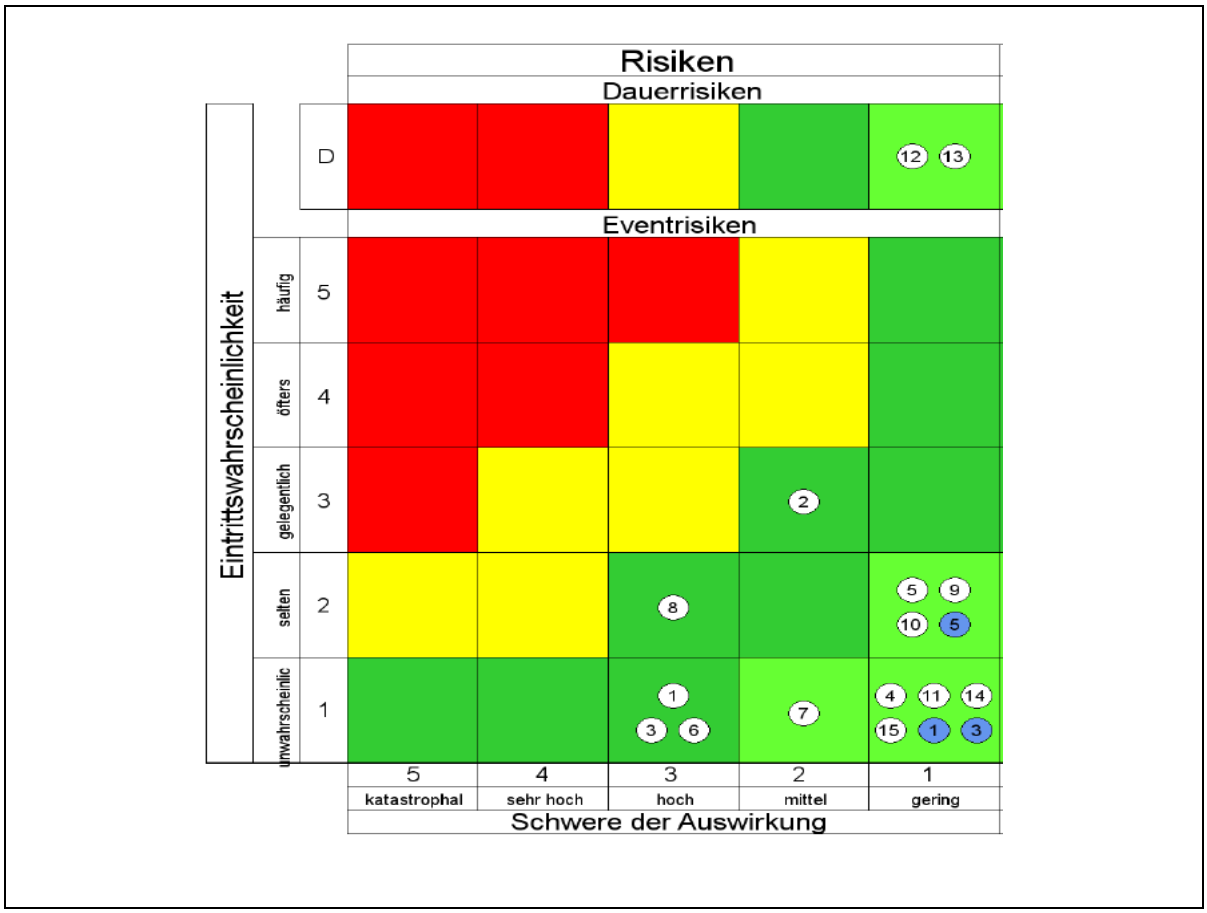


Abbildung 15: Aggregationsmatrix im "Best Case"

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

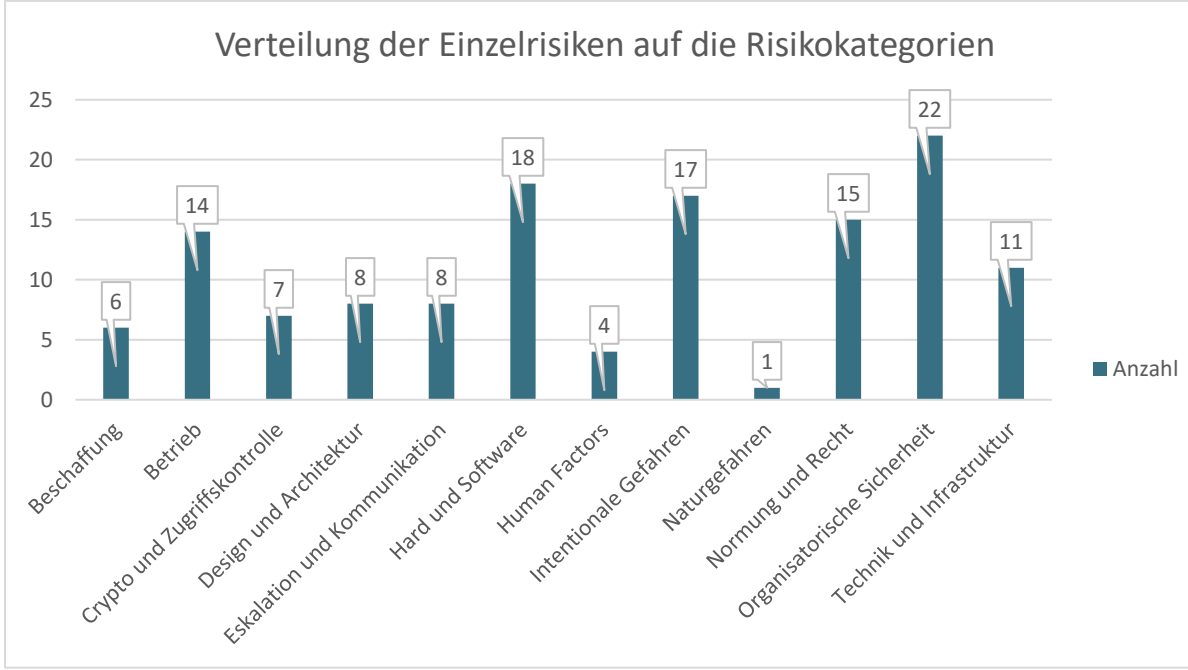


Abbildung 16: Darstellung der Verteilung der Risikokategorien

10. Gegenüberstellung der Veränderungen bei den Aggregationsrisiken

Im Wesentlichen gibt es folgende große Änderungen bei den Aggregationsrisiken:

- Das Aggregationsrisiko 15 ist neu hinzugekommen und beschäftigt sich mit dem Ausfall wesentlicher Betriebsmittel. Selbstverständlich liegt hier der Schwerpunkt auf der Stromversorgung. Die Einzelrisiken wurden dem Aggregationsrisiko Nr. 1 entzogen.
- Die Aggregationsbestandteile wurden zum Teil umgruppiert.
- Bei den betrieblichen Aspekten der Risikobewertung wurden im Vergleich zur Version 2.0-2019 keine Veränderungen vorgenommen.
- Die monetären Bewertungen wurden angepasst.

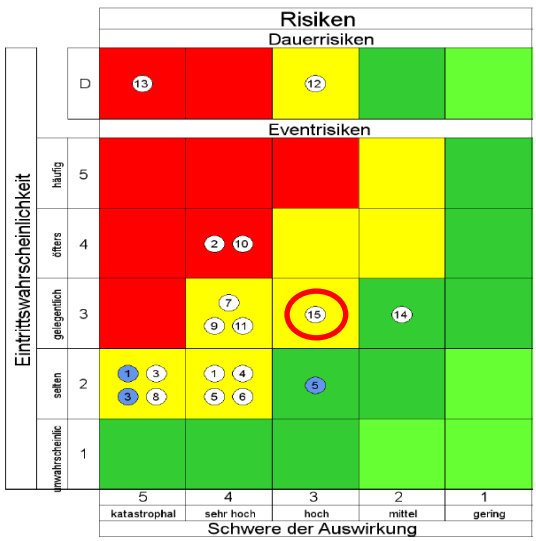


Abbildung 17: Aggregationsrisiken V3.0-2020

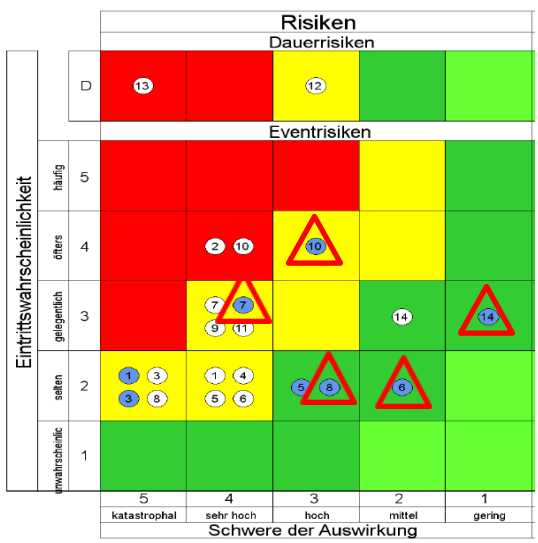


Abbildung 18: Aggregationsrisiken V2.0-2019

11. Zusammenstellung der Ergebnisse aus dem Workshop mit der E-Wirtschaft

Sowohl die Energiewirtschaft als auch die Telekommunikationsbranche hat im Vorfeld des ersten Informationsaustausches auf dieser Ebene eine Auswahl an Einzelrisiken, die Aggregationsrisiken sowie ein Exzerpt der Maßnahmen der jeweils anderen Branche zur Verfügung gestellt. Um ein gemeinsames Verständnis für die jeweiligen Risikobetrachtungen

zu schaffen, wurden in einem ersten Schritt die jeweiligen Risikokriterien gegenseitig vorgestellt.
Seitens der Energiewirtschaft wurden 17 vorausgewählte Einzelrisiken, die einen Bezug zur Telekommunikationsbranche haben könnten, detailliert dargestellt. Es ist jedoch zu betonen, dass es womöglich noch weitere „übereinstimmende" Risiken gibt. Im Ergebnis des **gesamten Workshops** werden zwei „Klassen" an Einzelrisiken definiert:

- G = Gemeinsames Risiko
- K = Kaskadenrisiko

Ein wesentlicher Aspekt in der begonnenen Diskussion war die Frage nach möglichen Kaskaden. Die Auswertung der Ergebnisse des Workshops mit der E-Wirtschaft sowie ein Review aller Einzelrisiken ergibt, dass bis dato **35 gemeinsame Risiken** identifiziert wurden. In Summe wurden **6 Risiken mit Kaskadenpotential** markiert und diskutiert.

Nr	Risikobezeichnung	Ursache	Wirkung	Kaskaden, gem. Risken
2	ITK-Leitungsunterbrechung in Verteilnetz	Techn. Gebrechen durch Baggerangriff, unsachgemäße Bauarbeiten, ggfs. vorsätzliche Handlungen	Erhebliche Störungen von 0 bis 80 % h	G, K
7	Regionaler Stromausfall	Technisches Gebrechen, Naturereignis	Ausfall der Dienstleitungen, verbunden mit erheblichem Wiederherstellungsaufwand bei Wiedereinschaltung	K
8	Flächendeckender Stromausfall für ein Bundesland, der über die Versorgungszeit von Notstrom/unterbrechungsfreier Stromversorgung hinausgeht	Technisches Gebrechen	Ausfall der Dienstleitungen, verbunden mit erheblichem Wiederherstellungsaufwand bei Wiedereinschaltung	K
53	Angriffe durch Stateactors/vergleichbar potente kriminelle Vereinigungen	Heterogene Motivationslage z. B. Sabotage, Industriespionage und monetäre Absichten + politische Absichten	Hoher Imageschaden, Zerstörung von IKT-Infrastruktur-Ausfall > 1920%h, damit verbundener monetärer Schaden, Abgriff schützenswerter Informationen	G, K-Cyberdefence Fall
109	Gefahr der mangelnden Koordination zwischen den Branchen zu IT-Security-Themen	Wahrung Betriebsgeheimnisse, Hemmnisse über Near-Misses zu berichten	zu späte Reaktion auf Schwachstellen, spätere Erkennung und längere Behandlungsdauer von Vorfällen, unvollständiges Lagebild	K
133	Gefahr der fehlenden Erfahrung im Umgang mit neuen Technologien	Erfahrungshorizont im Umgang mit den verschiedenen Authentifizierungsverfahren in 5G insbesondere WIFI-5G Access	unbekannte Angriffe auf die Verfügbarkeit, Authentizität und Integrität	G, K?

Tabelle 9: Risiken mit Kaskadenpotential

Man kann die Erkenntnisse hier wie folgt zusammenfassen:

- Technische Gebrechen wie eine Leitungsunterbrechung bei vermeintlichen Redundanzen, die jedoch physisch eng beieinanderliegen, können zu Kaskaden führen.
- Ein Stromausfall kann einerseits infolge der beschriebenen Szenarien auftreten, stellt aber auch allein eine entsprechende Herausforderung dar. Die Stromausfallszeiten sollten in einer eigenen Diskussionsrunde harmonisiert werden.
- Ausfall von Services und Dienstleistungen, sei er durch kriminelles Verhalten initiiert oder technisch-organisatorischer Natur, stellt einen wesentlichen negativen Aspekt möglicher Fehlerfortpflanzungen dar bzw. kann amplifizierende Schadwirkungen nach sich ziehen.
- Der wahrscheinlich am schwierigsten zu beherrschende Effekt ist der Umgang mit neuen Technologien. Hier wird einerseits sehr oft an neue Netztechnologien wie bspw. das 5G-Netz gedacht. Mangelnde Cybersecurity bei IoT-Devices könnte indirekt wieder Stromausfälle nach sich ziehen. Aber auch neue gesetzliche Rahmenbedingungen wie z. B. die Förderung der Stromerzeugung durch erneuerbare Energien, die in weiterer Folge einen deutlich erhöhten Mess- und Regelaufwand bedeutet, stellen neue, bis dato wenig bewertbare Kaskadenpotentiale dar.
- Kaskaden in Richtung Zeitsynchronisation können für den Handel und den Marktzugang ein Problem darstellen.
- Fehlender Informationsaustausch/BCM-Reife/Anforderungen an den Informationsbedarf der jeweils anderen Branche könnten in Zukunft auch mögliche Effekte mit Sekundärwirkungen auf die jeweils andere Branche nach sich ziehen. Daher wird empfohlen, dass das Austrian Energy CERT (AEC) bei entsprechenden Schadereignissen die TK-Branche mit einbindet.
- Kaskaden, die durch die vermehrte Nutzung von Clouddiensten entstehen, ziehen die klare Empfehlung nach sich, für die Versorgungssicherheit eigene Infrastrukturen vorzuhalten.

Teil IV Maßnahmen & Empfehlungen

12. Empfehlungen

Die nachfolgenden Empfehlungen leiten sich aus mehreren Perspektiven ab und fassen die Ergebnisse der Diskussionen in den elf Expertenworkshops in den beiden Jahr 2019-2020 zusammen. Die Empfehlungen stellen daher einerseits die Auswertungsergebnisse der gesamten Risikoanalyse zusammen und bilden andererseits aus technischer Sicht den kleinsten gemeinsamen Nenner für möglichst alle in der Branche vertretenen Stakeholder. Es werden daher

- die unmittelbaren Maßnahmen zur Risikominderung aus der Bewertung der Einzelrisiken zusammengestellt,
- die unmittelbar ausformulierten Maßnahmen aus der Bewertung der Aggregationsrisiken mitberücksichtigt,
- die für die Branche wichtigsten Entwicklungen aus einer **übergeordneten** Sicht

diskutiert und zugeordnet.

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

12.1 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 4.3)“, die kritische Infrastrukturen für Österreich betreiben, geführt. Diese Gruppe von Unternehmen / Organisationen werden im Sinne der hier vorliegenden Einteilung als KIs verstanden. Diese wurden seitens BMI/BKA bereits via Information an die Geschäftsleitung über ihren Status informiert bzw. werden laufend informiert.
Behörden sind per Definition eine „Kritische Infrastruktur“ in Österreich.

Die Kriterien für diejenigen Unternehmen, die der Gruppe der relevanten Systembetreiber zugeordnet wurden, werden in Abgrenzung zu den KIs bzw. Betreiber Wesentlicher Dienste gem. NISV in der Expertengruppe der RTR-IKT-Branchenrisikoanalyse festgelegt.

Unter diesen Betreibern werden jene meldepflichtigen Betreiber verstanden, die die Schwellwerte gemäß §3 TK-NSiV 2020 in den nachfolgenden Bereichen überschreiten können.

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

Empfehlungen an die relevanten Betreiber (SysB) richten sich selbstverständlich auch an die Kritischen Infrastrukturen bzw. Betreiber Wesentlicher Dienste.

Im Rahmen der Empfehlungen werden auch Prozesseigner definiert. Unter Prozesseigner im Sinne der Empfehlungen werden Organisationen verstanden, die die Umsetzung der Empfehlungen **federführend koordinieren** sollen.
Von den Prozesseignern wird erwartet, dass diese im Rahmen einer periodischen Revision der Umsetzung der Empfehlungen bzw. der Risikoanalyse selbst dem Lenkungsausschuss der RTR-IKT-Branchenrisikoanalyse den Umsetzungsstand darstellen und ggfs. Anpassungen vorschlagen.

12.2 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 Jahre benötigen

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

12.3 Übersicht der Empfehlungen

Aus den 12 Risikokategorien wurden 31 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
- » Business Continuity Management
- » Naturgefahren
- » Normung und Recht

Diese verteilen sich auf folgende Risikokategorien wie nachstehend abgebildet:

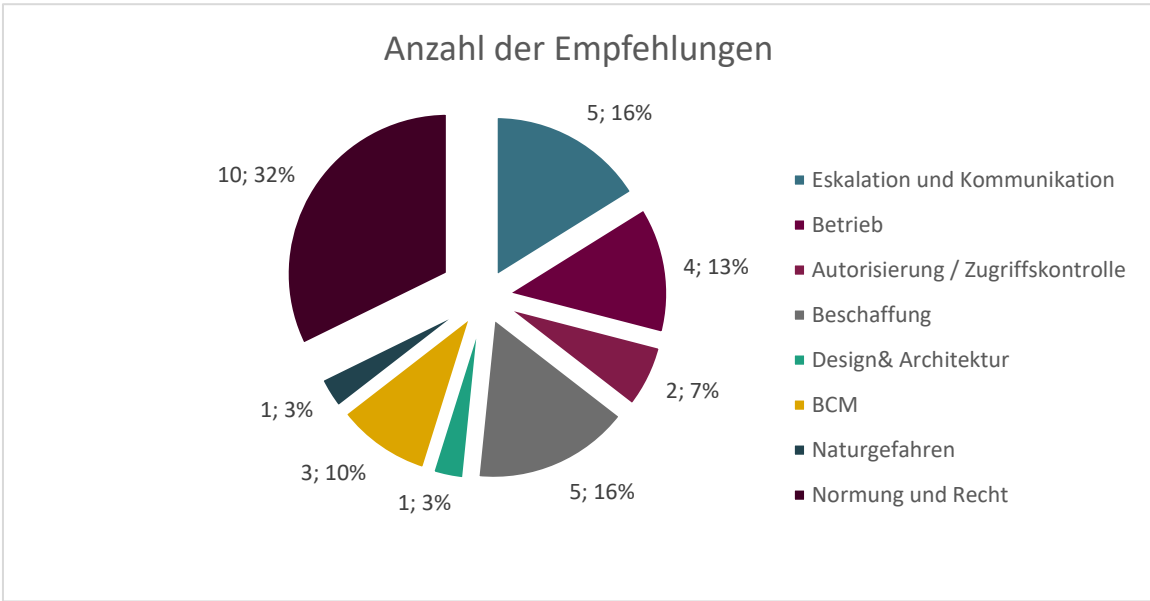


Abbildung 19: Verteilung der Empfehlungen auf die Risikokategorien

Abkürzungsverzeichnis

Abkürzungen	Beschreibung
(D) DOS	Distributed Denial of Service
APCIP	Österreichisches Prorgamm zum Schutz kritischer Infrastrukturen
APT	Advanced Persistent Threat
BCM	Business Continuity Management
BKA	Bundeskanzleramt
BM.I	Bundesministerium für Inneres
BSI	Bundesamt für Sicherheit in der Informationstechnik (Deutschland)
CERT	Computer Emergency Response Team
CPE	Customer Premises Equipment
CSP	Cyber Sicherheit Plattform
ENISA	Agentur der Europäischen Union für Cybersicherheit
EPCIP	European Programme for Critical Infrastructure Protection
IM	Incident Management
IoT	Internet of Things
IS	Internetservices
ISMS	Informationssicherheitsmanagementsystem
ISO	Internationale Organisation für Normung
ISP	Internetserviceprovider
ISPA	Internet Service Providers Austria
KI	Kritische Infrastrukturen
KRITIS	Kritische Infrastrukturen
LSA	Lenkungsausschuss
NIS	Netz- und Informationssystemsicherheit
NISG	Netz- und Informationssystemsicherheitsgesetz
NISV	Netz- und Informationssystemsicherheitsverordnung
ONR	Österreichische Normenregel (ON-Regel)
OS	Betriebssystem (Operating System)
ÖSCS	Österreichische Strategie für Cyber Sicherheit
PDCA	Plan Do Check Act
PKI	Public Key Infrastructure
PPP	Public-private-Partnership
RED	Radio Equipment Directive
SKKM	Staatliches Krisen und Katastrophenschutzmanagement
TELKO	Telekommunikationsprovider
TK	Telekommunikation
USV	Umfassende Sicherheitsvorsorge

Quellenverzeichnis

- Lit.RTR-01, Schwachstelle im Mobilfunknetz: Kriminelle Hacker räumen Konten leer
- Lit.RTR-02, The Fall of SS7 - How Can the Critical Security Controls Help?
- Lit.RTR-03, NISG, Bundesgesetz zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystemsicherheitsgesetz – NISG), https://www.ris.bka.gv.at/GeltendeFassung/Bundesnormen/20010536/NISG%2c%20Fassung%20vom%2021.10.2020.pdf
- Lit.RTR-04, Zuordnungstabelle ISO 27001 sowie ISO 27002 und IT-Grundschutz
- Lit.RTR-05, Security Profiles ISPA AG Security
- Lit.RTR-06, Study on Mobile Device Security
- Lit.RTR-07, Cyber-Risiken Österreich 2016
- Lit.RTR-08, Report Cyber-Risikomatrix
- Lit.RTR-09, Assessing Threats to Mobile Devices & Infrastructure - The Mobile Threat Catalogue
- Lit.RTR-10, Digitaler Stillstand - Die Verletzlichkeit der digital vernetzten Gesellschaft
- Lit.RTR-11, Critical Security Controls V6.0 CIS TOP 20
- Lit.RTR-12, 7 Layers of OSI
- Lit.RTR-13, Annual Incident Reports 2015 - Analysis of Article 13a annual incident reports in the telecom sector
- Lit.RTR-14, ENISA Guideline on Threats and Assets - Technical guidance on threats and assets in Article 13a (Version 1.2 08/2015), https://www.enisa.europa.eu/publications/technical-guideline-on-threats-and-assets
- Lit.RTR-15, Risk management and risk profile guidelines for telecommunication organizations
- Lit.RTR-16, ITU-T X.1051 (04/2016) SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY Information and network security – Security management. Information technology – Security techniques - Code of practice for information security controls based on ISO/IEC 27002 for telecommunications organizations
- Lit.RTR-17, ITU-T X.1055 (11/2008), SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY Telecommunication security. Risk management and risk profile guidelines
- Lit.RTR-18, Technische Sicherheitsanforderungen - Kompendium für technische Projektleiter und Entwickler
- Lit.RTR-19, Extremszenario - Physiker warnen vor Super-Sonnensturm
- Lit.RTR-20, Bundesgesetz über die Organisation der Sicherheitsverwaltung und die Ausübung der Sicherheitspolizei (Sicherheitspolizeigesetz – SPG)

» Lit.RTR-21, Bundesgesetz, mit dem ein Telekommunikationsgesetz erlassen wird (Telekommunikationsgesetz 2003 –TKG 2003)

» Lit.RTR-22, CYBER; Implementation of the Network and Information Security (NIS) Directive

» Lit.RTR-23, Cybersecurity Act

» 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)

» Lit.RTR-25, Digitalstrategie der Europäischen Kommission, https://ec.europa.eu/info/sites/info/files/strategy/decision-making_process/documents/ec_digitalstrategy_de.pdf

» Lit.RTR-26, ENISA Threat Landscape for 5G Networks (11/2019), https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks

» Lit.RTR-27, NIS-Fact Sheet 08/2019, https://www.nis.gv.at/NIS_Fact_Sheet_8_2019_1.0.pdf

» Lit.RTR-28, Netz- und Informationssystemsicherheitsverordnung, NISV

» Lit.RTR-29, Richtlinie 2014/53/EU des Europäischen Parlaments und des Rates vom 16. April 2014 über die Harmonisierung der Rechtsvorschriften der Mitgliedstaaten über die Bereitstellung von Funkanlagen auf dem Markt und zur Aufhebung der Richtlinie 1999/5/EG

» Lit.RTR-30, Empfehlung (EU) 2019/534 der Kommission vom 26. März 2019, Cybersicherheit der 5G-Netze, https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX:32019H0534

» Lit.RTR-31, Bericht IKT Branchen Risikoanalyse Version 1.0 (RTR-Release to Public 02/2018), https://www.rtr.at/de/tk/TKBranchenrisikoanalyse2018

» Lit.RTR-32, EU coordinated risk assessment of the cybersecurity of 5G networks (Report 10/2019), https://ec.europa.eu/digital-single-market/en/news/eu-wide-coordinated-risk-assessment-5g-networks-security

» Lit.RTR-33, Cybersecurity of 5G networks EU Toolbox of risk mitigating measures (NIS CG Publication 01/2020), https://ec.europa.eu/digital-single-market/en/news/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures

» Lit.RTR-34, Netz- und Informationssystemsicherheitsverordnung – NISV (BGBl. II Nr. 215/2019), https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20010722

» Lit.RTR-35, Telekom-Netzsicherheitsverordnung 2020 - TK-NSiV 2020 (BGBl. II Nr. 301/2020), https://www.rtr.at/de/tk/TK_NSiV_2020

» Lit.RTR-36, 3GPP TS 33.501: Security architecture and procedures for 5G System, https://www.3gpp.org/DynaReport/33501.htm