Rundfunk & Telekom Regulierungs-GmbH

Bericht

IKT Branchenrisikoanalyse

Version 4.0-2024

RTR-TLP-CLEAR

Auftraggeber: RTR GmbH	Gesamtzahl Seiten: 109
Aufgabensteller: Mag. U. Latzenhofer	Anzahl Tabellen: 19
Studienkennziffer: entfällt	Anzahl Abbildungen: 18

Wien, 26.06.2024

Koordinierender Verfasser: DI Wolfgang Czerni, MBA

Management Summary

Die vorliegende Version der 4.0-2023-IKT-Branchenrisikoanalyse folgt dem durch den Lenkungsausschuss festgelegten Reviewzyklus und baut auf Version 3.0-2020 auf. Die Evaluation der Risiken fand in einem PPP-Prozess unter Mitwirkung von Ministerien, der Regulierungsbehörde RTR, Festnetz- und Mobilfunkbetreibern und dem CERT.AT statt.

Damit erfüllt die Branchenrisikoanalyse alle Schwerpunkte der Umsetzung der Österreichischen Cyber Sicherheitsstrategie 2021. Vor allem da es während deren Entwicklung zwei Workshops mit Expert*innen aus der Energiebranche gab und sich die beiden Regulierungsbehörden RTR und E-Control Austria koordiniert haben.

Im Rahmen der Expert*innen Workshops wurden auch die Schnittstellen zur kommenden RKE Richtlinie diskutiert. Dazu wurden Vertreter aus dem BMI eingeladen. Aktuelle Entwicklungen aus der NIS-Cooperation Group sowie weitere Arbeiten auf der EU-Ebene wie zum Beispiel Cyber Resilience Act wurden von Expert*innen aus dem BKA, der strategischen NIS Behörde präsentiert.

In Summe wurden 7 Workshops à 4h dazu genutzt, die bereits erfassten Einzelrisiken zu evaluieren und neu zu bewerten. Die Einzelrisiken sowie ad hoc Schwerpunktthemen wie z.B. „Identifikation und Festlegung von Hochrisikolieferanten“ münden in einer Aggregationsrisikomatrix, die 15 aggregierte Risiken und einen Empfehlungskatalog mit 28 Empfehlungen enthält. Während der Genese der V3.0-2020 lag der Fokus der Risikobetrachtungen auf der Einführung der 5G Netze.

Die vorliegende Version steht im Spannungsfeld der bereits implementierten Sicherheitsmaßnahmen aus dem NISG, TKG und der kommenden Umsetzung zur NIS2 Richtlinie. In der aktuellen NIS/TKG Gesetzgebung wird noch von Sicherheitsmaßnahmen gesprochen. Die NIS2 schreibt Risikomanagementmaßnahmen vor. Genau hier setzt die Branchenrisikoanalyse an und formuliert de facto einen Risikomanagementprozess. Die genaue Ausgestaltung der Risikomanagementmaßnahmen basierend auf NIS2 sind noch nicht bekannt. Da sich die Risikoanalyse aber nach dem Stand der Technik richtet, in dem die Vorgaben der ISO 31.000, *risk management* bzw. ÖNORM S2412ff, *Risikomanagement*“ berücksichtigt werden, sollte der Anschluss an NIS2 möglich sein.

Dass die Ziele der Gesetzgebung bereits erste Ergebnisse zeigen, manifestiert sich auch in der Risikoanalyse. Die gemeinsamen Anstrengungen der Branche zeigen hier Wirkung. In der Version 3.0-2020 wurden 131 Einzelrisiken erfasst und bewertet. 21 Risiken davon konnten aufgrund der mitigierenden Maßnahmen bereits gestrichen werden. Substantiell wurden drei Risiken jedoch neu hinzugefügt, die sich aus der geänderten allgemeinen politischen Sicherheitslage und der gestiegenen Kriminalitätsaktivität im Cyberraum ergeben. Auch die Risikoverteilung hat sich verschoben. Es wurden im Vergleich zur Vorversion die Einzelrisiken in ihrer Risikohöhe im Schnitt deutlich hin zu Risiken mittlerer Risikohöhe verschoben. Wurden 2020 19% der Risiken noch als hoch eingestuft, sind im Vergleich dazu aktuell nur mehr 7% als hoch bewertet. Das bedeutet, dass Cyberkriminalität für die Branche

als ein hohes Dauerrisiko eingestuft wird, da die Häufigkeit, Intensität und „Qualität“ im Beobachtungszeitraum zugenommen hat.

2020 wurden 31 Empfehlungen formuliert. Aufgrund der sich veränderten Gesetzlage konnten auch hier drei Empfehlungen als „bereits umgesetzt“ gestrichen werden, da sie durch gesetzliche Auflagen geregelt sind.

Das gesamte erfasste Risikoportfolio basiert auf über 500 strukturiert erfassten Gefahren, die nach verschiedenen Gesichtspunkten der Informationssicherheit in der TELKO und ISP Branche strukturiert sind.

Im Ergebnis kann man zusammenfassen, dass sich die Schwerpunkte der Risikolandschaft - abgesehen von den ständigen Herausforderungen bei Design und Architektur sowie bei Hard und Software - hin zur Bewältigung von qualitativ anspruchsvollen bis sehr speziellen Cybercrime Szenarien entwickelt haben.

Zur Mitigation solcher Szenarien bedarf es eines dualen Ansatzes. Einerseits die Intensivierung des Informationsaustausches zwischen den Branchen und andererseits gesetzliche Rahmenbedingungen, die einen solchen Austausch auch erlauben.

Abgeleitet daraus werden vier zentrale Empfehlungen als prioritär angesehen:

- ein Sektor übergreifender Informationsaustausch zwischen Betreibern und Behörden zur Bekämpfung bzw. Eindämmung von Cyberbedrohungen und dem dadurch verursachten Schaden soll rechtlich ermöglicht und technisch beschleunigt werden.
- Die Branchen übergreifende Zusammenarbeit zur Steigerung der Resilienz soll weiter ausgebaut werden.
- Im nächsten Reviewzyklus muss die Risikoanalyse die Vorgaben der NIS2 berücksichtigen. Dazu sollten in Vorbereitung auf die bereits angesprochenen Risikomanagementmaßnahmen die zusammengestellten Risiken in einer strukturierten Form auch mit anderen Branchen harmonisiert werden.
- Das Risikoportfolio der Branchenrisikoanalyse sollte in die geplanten Vorgaben zur Präzisierung der NIS2 Risikomanagementmaßnahmen eingearbeitet werden. Da dazu seitens BMI und BKA Branchenworkshops geplant sein sollen, muss die RTR hier eine koordinierende Rolle für IKT Betreiber übernehmen.

Kurzfassung

Der vorliegende Bericht fasst die Ergebnisse der vorliegenden Version 4.0-2023 der RTR-IKT-Branchenrisikoanalyse im Zeitraum von April bis November 2023 zusammen. Im Wesentlichen werden vier Schwerpunkte beschrieben.

Im Teil I werden die Methodik und Vorgehensweise, kurz wiederholend, zur Version 3.0 dargestellt. Teil II fasst die geänderten Rahmenbedingungen für den hier dargestellten Risikomanagementprozess zusammen. Insbesondere der Ausblick auf die Einführung bzw. Umsetzung der NIS2-Richtlinie. Teil III widmet sich der Darstellung und Diskussion der wesentlichen Ergebnisse wie Gefahrenkataloge, Einzel- und Aggregationsrisiken und Einarbeitung der *lessons identified* aus den letzten drei Jahren sowie aus den gewonnenen Erkenntnissen der Einführung der 5G-Technologie. Der Teil IV beschäftigt sich mit den abgeleiteten übergeordneten Empfehlungen zur Weiterentwicklung der Cybersicherheit bei allen Stakeholdern.

In Summe wurden in fünf jeweils ca. vier Stunden dauernden Arbeitsworkshops die 131 Einzelrisiken aus Version 3.0-2020 überarbeitet. Hier wurden 21 Einzelrisiken entweder gestrichen oder durch Schärfung der Risikobezeichnung, Ursachenbeschreibung und Auswirkung zu 110 Einzelrisiken bewertet. In der Analyse wurden drei neue Einzelrisiken identifiziert und zu einem Risikoprofil bestehend aus 113 Einzelrisiken hinzugefügt. Diese Bewertung fand auf Basis des - in der Version 3.0-2020 aktualisierten und in der Branche abgestimmten 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. Die in diesem Prozess identifizierten Risiken 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 Internetservicedienstleistungen gegenüber den rein finanziellen Risiken für die jeweilige Organisation im Vordergrund steht. Wenngleich auch in den Aggregationsrisiken zusätzliche monetäre Bewertungen mit aufgenommen wurden.

Alle Risiken wurden in einem „Worst Case“, einem „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 Schadensereignisse, die ständig bzw. mit sehr hohen Frequenzen auftreten, auf einer eigenen Risikoachse dargestellt (Dauerrisiken).

Für die Darstellung der 15 Aggregationsrisiken wurde der „Worst-Case“ Fall herangezogen. Es wurden für die Betrachtung vier hohe, 10 mittlere und ein geringes Risiko identifiziert.

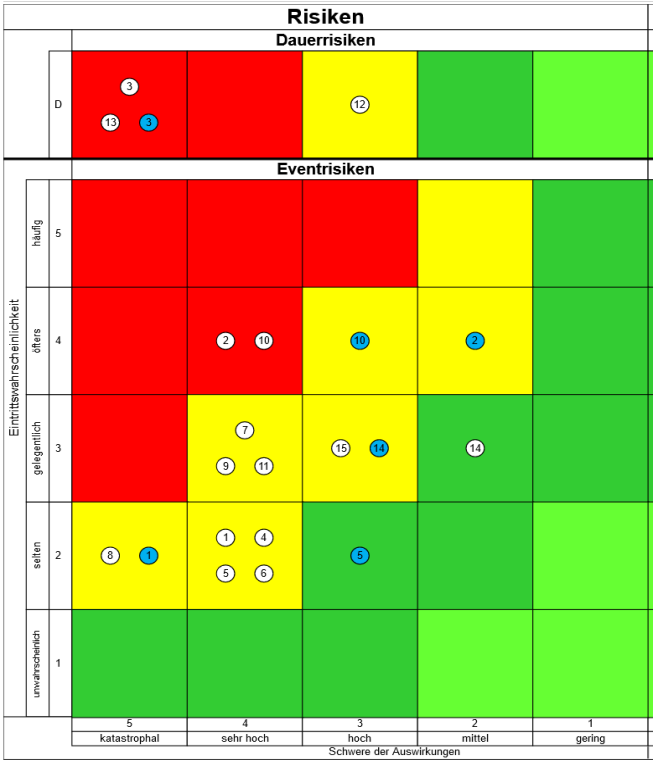

Abbildung 1: Aggregationsrisiken Übersicht

Weiß umrandete Zahlen wurden betrieblich-technisch bewertet.
Blaue Risiken wurden aus monetärer Sicht bewertet.

- 03, kriminelle Handlungen aus dem Cyberraum sowie Cyber-Fraud
- 13, Verwundbarkeiten bei Hard- und Software
- 02, Gefahr der Beschädigung oder Zerstörung oder Diebstahl wichtiger physischer Betriebsmittel
- 10, Verlust der Vertraulichkeit von geschützter Information
- 01, Ausfall wesentlicher Infrastrukturen oder Betriebsmittel
- 04, Mögliche, erhebliche Defizite bei IKT-Design und Systemarchitektur
- 05, negative Auswirkungen von politisch/rechtlichen Vorgaben aufgrund sich ändernden Rahmen-bedingungen auch öffentliche Wahrnehmung
- 06, Unzureichende Berücksichtigung von ISMS-Anforderungen im Beschaffungsprozess
- 07, Mangelhaftes Notfall-, Krisen- und Kontinuitäts-management
- 08, Erhebliche Probleme beim Patch- und Update-Prozess
- 09, Defizite bei Identity and user access control (IAM)
- 11, Ausfall oder erhebliche Serviceeinschränkungen bei singulären IKT-Lieferanten oder Herstellern
- 12, Mängel in der Betriebsführung
- 13, Vulnerabilities bei Hard- und Software
- 15, Ausfall der übergeordneten Stromversorgung (Energiemangellage)
- 14, Mangelnde Compliance (Datenschutz, Standards, Verträge etc.) oder fehlende Legistik

Die in der Matrix blau gefärbten Risiken wurden in monetärer Hinsicht bewertet.

Risiko Nr. 3 wurde in dieser Version wegen der gestiegenen Häufigkeit und Qualität der Cybercrime Szenarien zu einem Dauerrisiko hochgestuft. Das Dauerrisiko Nr. 13, beschäftigt sich mit den nach wie vor hohen Herausforderungen und Abhängigkeiten von Lieferanten und Herstellern bei der „Qualität“ in technischer Hinsicht, aber auch bei Security Aspekten im Betrieb. Das Risiko Nr. 2 fokussiert in Abgrenzung zu Risiko Nr.3 primär auf physische Angriffe bzw. Gefahren für die IKT-Infrastrukturen. Nr. 10 beschreibt die hohen Risiken für schützenswerte Informationen, die auf IKT verarbeitet und gespeichert werden.

Die Einzelrisiken wurden in 12 Risikokategorien zusammengefasst. Innerhalb dieser Risikokategorien wurden 28 Empfehlungen erarbeitet, die mehreren IKT-Branchen-Stakeholdern zugeordnet wurden. Um die Maßnahmenumsetzung und Verfolgung zu erleichtern, hat die Expert*innengruppe für alle Empfehlungen einen Prozesseigner vorgeschlagen. Dieser sollte in drei bereits vordefinierten Prognosehorizonten die Umsetzungen der Empfehlungen koordinieren bzw. katalysieren. Der Horizont wurde so

gewählt, dass die mit Oktober 2024 geltenden Regelungen aus NIS2 berücksichtigt werden können. Zu jedem Einzel- und Aggregationsrisiko wurden Minimierungsmaßnahmen vorgeschlagen. Viele davon sind in den meisten Unternehmen bereits initiiert oder umgesetzt.

Die Aggregationsrisiken wurden aus betrieblicher Sicht in ihrer Risikohöhe bestätigt. Es wurde lediglich das Risiko Nr. 3 zu einem Dauerrisiko erklärt, wobei sich die Aggregationszuordnungen verändert haben und damit auch die Schwerpunkte der Risiken. Die monetären Bewertungen, blaue Kreise bzw. schwarze Dreiecke, wurden überarbeitet.

In der V3-2020 war ein Schwerpunkt auf der Einführung der 5G-Technologie gelegt worden.

Obwohl die meisten Aggregationsrisiken hier unverändert erscheinen, wurden bei den Einzelrisiken 21 Risiken gelöscht und 3 Einzelrisiken hinzugefügt.

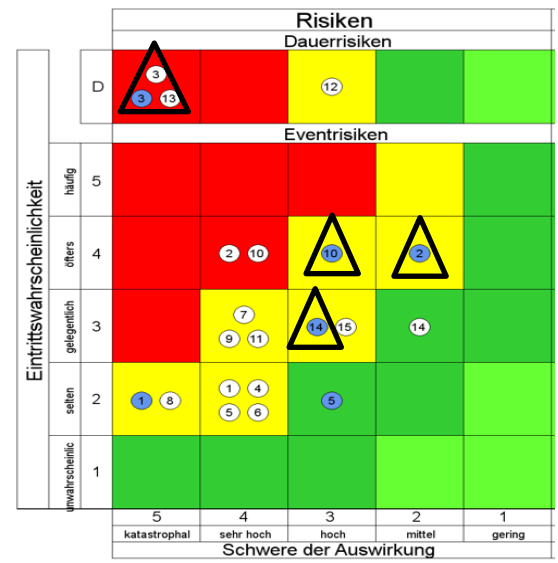

Abbildung 2: Aggregationsrisiken V4.0-2023

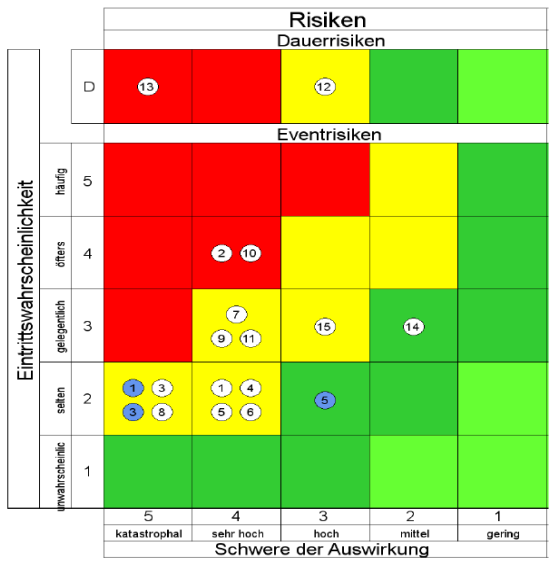

Abbildung 3: Aggregationsrisiken V3.0-2020

Die Ergebnisse wurden in einer Expert*innengruppe, bestehend aus Branchenvertreter*innen verschiedener Organisationsgrößen, der Interessensvertretung der Internetserviceprovider in Österreich sowie unter aktiver Beteiligung von BMF, BMI, BKA, CERT.at und der RTR erarbeitet.

Die Workshops wurden in Form 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 V3.0-2020 aufgebaut. Sie liegt in vier Teilen vor:

- Teil I beschreibt die allgemeine Herangehensweise und Methode zur Risikoidentifikation und Bewertung. Die Vorgehensweise orientiert sich an den Vorgaben der „ISO 31.000 risk management", „ISO 31.010 risk assessment techniques" und der ONR 49.002-2, Risikomanagement für Organisationen und Systeme, Leitfaden für die Methoden der Risikobeurteilung.
- Der Teil II, Kontexterfassung, befasst sich mit der Einbettung der Branchenrisiko-analyse in die nationalen und internationalen Programme und Vorgaben zur Cybersicherheit, u. a. der NIS[1]-Richtlinie, NISG[2], NISV oder der TK-NSiV 2020 auf Basis der Grundlagen des §44 TKG (2021), idgF.
- Im Teil III, Ergebnisdarstellung, werden die aktuellen Anpassungen und Erweiterungen des Risikoportfolios der Branche zusammengestellt.
- 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 eines Privat-Public-Partnership-Programms (PPP) verstanden. Eine wiederkehrende Evaluierung der Ergebnisse ist daher notwendig. Die Periodizität orientiert sich an den Zertifzierungszyklen einschlägiger Normen wie z.B. der ISO 27.001. Arbeitsaufträge werden durch den Lenkungsausschuss determiniert und im Rahmen von Expert*innenworkshops umgesetzt.

Die Aktualisierung wurde in fünf ca. vier bis fünf Stunden dauernden Workshops beginnend im Frühjahr 2023 durchgeführt.

Für die vorliegenden Betrachtungen, insbesondere für die Zusammenstellung der Empfehlungen wurde ein Prognosehorizont bis 2026 vereinbart. Dieser Prognosehorizont leitet sich zwingend von der Inkraftsetzung der NIS2 Gesetzgebung ab.

[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] 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 neuen Gefahren und die damit verbundenen Risiken durch Einführung bzw. Implementierung von neuen Technologien.
- 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 der vorangegangenen Evaluierungsschritte begonnen und ist fortzusetzen.

Ein weiteres Ziel ist die „Annäherung" der Branchenrisikoanalyse an die künftigen Anforderungen aus NIS2. Hier wird grundsätzlich der Begriff „Risikomanagement-maßnahmen" anstatt Sicherheitsmaßnahmen verwendet. Die genauen Ausgestaltungs-vorgaben dieser Risikomanagementmaßnahmen stehen noch nicht fest.

Fakt ist, dass das NISG die Implementierungen von Informationssicherheitsmanagement-systemen oder vergleichbaren Managementsystemen katalysiert hat, 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 Internetservice-provider 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 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 abgeschätzt werden. Wie bereits erwähnt, wurde der Prognosehorizont für die Erfassung und Bewertung von Risiken mit 2026 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[3]. Um dem PPP-Gedanken entsprechend Rechnung zu tragen, wurde 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-21), zur Österreichischen Sicherheitsstrategie (USV), zur Cybersecurity Plattform (CSP) und zum Österreichischen Programm zum Schutz kritischer Infrastrukturen (APCIP) darstellt.
- Ein erweitertes Projektteam von Expert*innen bei TELKOs und ISPs sowie deren Interessensvertretung (ISPA) und CERT.at

[3] Siehe ÖNORM S4902-1-2-3, ISO. 31.000 und ISO 31.010

3.1 Übersicht Risikoidentifikations- & Bewertungsprozesses

Der Risikoerfassungs- und Bewertungsprozess wurde gemäß Abbildung 4 durchgeführt.

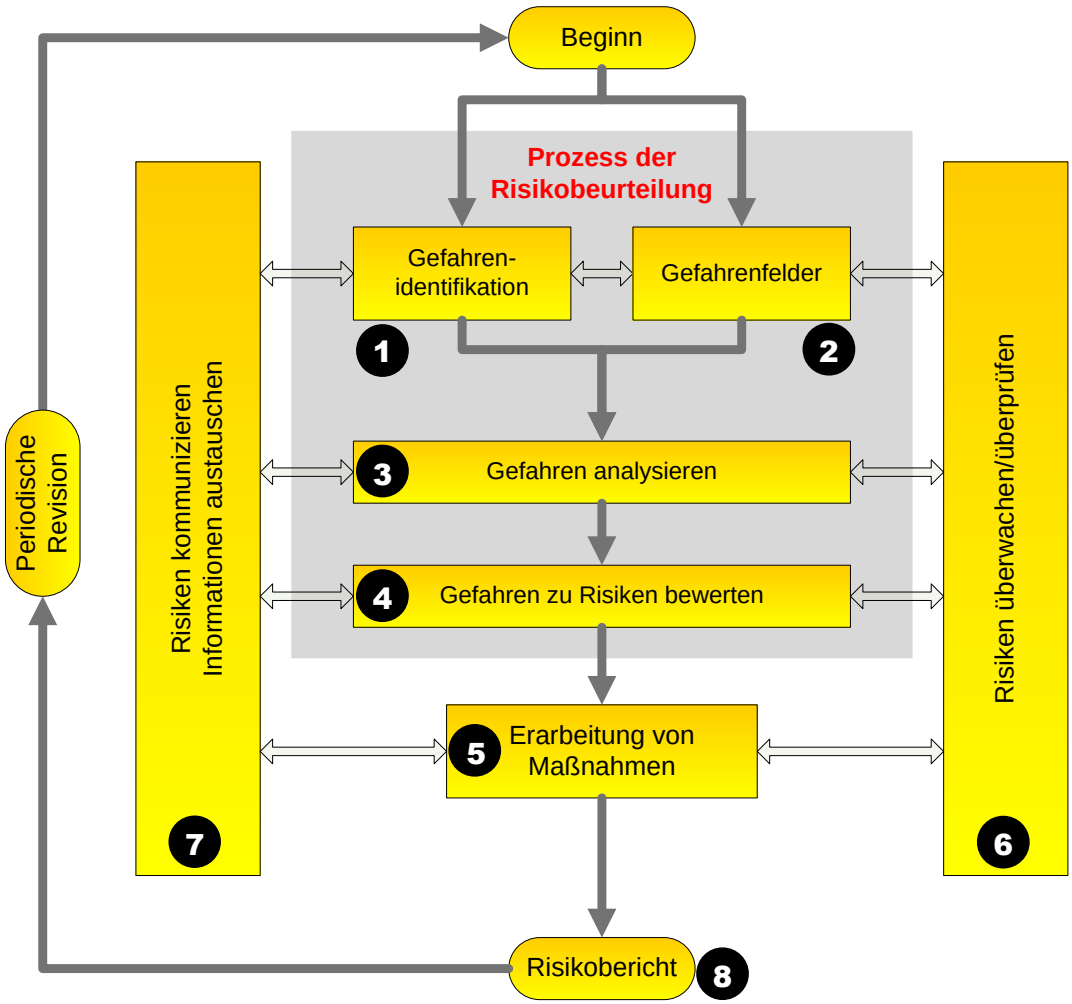

Abbildung 4: Vorgehensweise in der Risikoanalyse

3.1.1 PROZESSSCHRITT 1, GEFAHRENIDENTIFIKATION

Der Gefahrenidentifikationsprozess geht davon aus, dass Kommunikation in Form von Sprache und Daten in den 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 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-Grundschutzkataloge (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 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 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 5)
- Phase II, Bewertung der 526 identifizierten Gefahren zu 113 Einzelrisiken, wobei die Risiken in mehrfacher Hinsicht bewertet wurden. Einerseits einmal in der 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 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. Grundsätzlich wurde versucht, bei allen Einzelrisiken und 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 11.11.2023 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. Die Österreichische Cyber Sicherheitsstrategie ÖSCS

Die ÖSCS 2021 baut auf der Österreichischen Sicherheitsstrategie (ÖSS) auf und ist eine Weiterentwicklung der ÖSCS 2013. Sie zielt im Wesentlichen darauf ab, Sicherheit für die digitale Infrastrukturen zu schaffen bzw. zu gewährleisten. Es wurde der Rahmen für die wesentlichsten Grundlagen und Prozesse für den Aufbau einer umfassenden und zusammenhängenden Cybersicherheitspolitik für Österreich in einer Strategie veröffentlicht.

Mit dem Inkrafttreten der NIS-Richtlinie[4] (NIS-RL) wurde zum ersten Mal ein umfassender Rechtsakt über Cybersicherheit in der EU geschaffen. Im Zentrum steht dabei die Definition von einheitlichen Sicherheitsstandards und Meldewegen für all jene Unternehmen, die für das Funktionieren des Binnenmarktes und damit der Staaten essentiell sind. In Österreich wurde die NIS-RL durch das Netz- und Informationssystemsicherheitsgesetz (NISG) umgesetzt. Damit wurden nicht nur einheitliche Sicherheitsanforderungen für Unternehmen der kritischen Infrastruktur festgelegt, sondern auch erstmals die Erstellung einer Cybersicherheitsstrategie gesetzlich verankert. Die Branchenrisikoanalyse erfüllt somit alle 5 Punkte der Umsetzungsschwerpunkte der Österreichischen Sicherheitsstrategie die

1. **Sicherheitsgedanke:** Der Betrieb und die Weiterentwicklung der IT hat auf einem umfassenden Sicherheitsgedanken zu basieren, der strategische, organisatorische und technische Elemente (z. B. Security by Design) berücksichtigt. Dabei ist ein gemeinsames Vorgehen der Ressorts herzustellen.
2. **Risikobasierter Ansatz:** Die ÖSCS 2021 geht von einem gesamtheitlichen und risikobasierten Ansatz aus. Dieser zielt darauf ab, die wahrscheinlichsten und folgenschwersten Risiken zu identifizieren, zu priorisieren und entsprechende Gegenmaßnahmen zu entwickeln.
3. **Transparenz:** Bei der Umsetzung von Maßnahmen wird der Ansatz der Transparenz verfolgt, indem der Maßnahmenkatalog und der Fortschrittsbericht – soweit möglich – veröffentlicht werden.
4. **Kooperativer Ansatz:** Die relevanten Akteure arbeiten gemeinsam an der Umsetzung von konkreten Maßnahmen.
5. **Multi-Stakeholder-Ansatz:** Im kooperativen Ansatz sollen die betroffenen Interessensgruppen – soweit möglich – eingebunden werden und aktiv mitgestalten können. Die Komplementarität staatlicher und nichtstaatlicher Maßnahmen ist dabei wesentlich.

[4] Richtlinie (EU) 2016/1148 vom 6.7.2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (NIS-RL)

4.1 Umsetzung von NISG und NISV

Mit dem 2013 veröffentlichten Vorschlag für eine „Richtlinie des Europäischen Parlaments und des Rates vom 06.07.2016 über Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit in der Union", kurz NIS-Richtlinie muss Österreich die Vorgaben dieser Richtlinie bis zum 09. Mai 2018 umsetzen. Die Umsetzung erfolgte mittels des Bundesgesetzes zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystemsicherheitsgesetz – NISG, BGBl I Nr. 111/2018) und der unmittelbar zugeordneten Verordnung NISV (BGBl II Nr. 215/2019). Dieses ist am 1. Juli 2020 in Kraft getreten. Im NISG wird auch der Kontext zum TKG geregelt. Im Wesentlichen betrifft die Telekommunikationsbranche jedoch gemäß NISV, der §10, Betreiber (wesentlicher) digitaler Dienste.

Mit dem Inkrafttreten des NISG bzw. der NISV, wurden 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 Sicherheitsstandards ist mit dem §44 TKG 2021 zu Sicherheitsvorfällen klar abgegrenzt.

Am 04.07.2020 trat die Telekom-Netzsicherheitsverordnung 2020 („TK-NSiV 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.

Mit Bezug auf die Branchenrisikoanalyse 3.0-2020 stellt die Verordnung spezifische Anforderungen an Betreiber von 5G-Netzen mit mehr als 100.000 Teilnehmern in allen von ihnen betriebenen Netzen auf und setzt damit einige der Vorgaben aus der 5G EU Toolbox um. In der V3.0-2020 wurden mögliche Risiken eingehend analysiert. Diese werden im Rahmen der vorliegenden Version V4.0-2023 weiter evaluiert bzw. neu bewertet.

4.2 NIS2 & TKG

Die Regelungen aus NIS2 treten aller Voraussicht nach ab Oktober 2024 in Kraft. Der bisherige Anwendungsbereich der NIS-Richtlinie nach Sektoren wird mit NIS2 auf einen **weit größeren Teil der Wirtschaft** ausgeweitet, um eine umfassende Abdeckung der Sektoren und Dienste zu gewährleisten, die in Österreich für *„grundlegende gesellschaftliche und wirtschaftliche Tätigkeiten von entscheidender Bedeutung sind"*.

Betroffen sind große und mittlere Unternehmen aus folgenden Sektoren:

Unternehmen mit hoher Kritikalität:	Sonstige kritische Sektoren:
» Energie » Verkehr » Bankwesen » Finanzmarktinfrastrukturen » Gesundheitswesen » Trinkwasser » Abwasser » **Digitale Infrastruktur** » Verwaltung von IKT-Diensten B2B » öffentliche Verwaltung » Weltraum Die Kritikalitätsparameter sind im Anhang I der Richtlinie definiert.	» Post- und Kurierdienste » Abfallbewirtschaftung » Chemie » Lebensmittel » verarbeitendes/herstellendes Gewerbe » Anbieter digitaler Dienste » Forschung (fakultativ) Diese werden im Anhang II der Richtlinie definiert

Betroffene Organisationen müssen geeignete **Risikomanagementmaßnahmen** für die Sicherheit ihrer Netz- und Informationssysteme treffen und unterliegen Meldepflichten.

Es wird dabei zwischen **Wesentlichen Einrichtungen**, die ex ante einer Aufsicht nach Art 32 Abs. 2 Lit. b NIS2-RL unterliegen werden und **Wichtigen Einrichtungen,** die einer ex post Aufsicht nach Art 33 Abs. 2 Lit.b unterliegen.

Für „Digitale Infrastrukturen" laut Anhang I gibt es gesonderte Regelungen.

<table>
<tr><th>Art der Einrichtung</th><th>groß</th><th>mittel</th><th>klein</th></tr>
<tr><td>TLD-Namenregister</td><td colspan="3" rowspan="3">wesentlich</td></tr>
<tr><td>Qualifizierte Vertrauensdiensteanbieter</td></tr>
<tr><td>DNS Diensteanbieter (ausgenommen Betreiber von Root Nameserver)</td></tr>
<tr><td>Anbieter öffentlicher elektronischer Kommunikationsnetze oder elektronischer Kommunikationsdienste</td><td colspan="2">wesentlich</td><td>wichtig</td></tr>
<tr><td>Vertrauensdiensteanbieter</td><td rowspan="5">wesentlich</td><td colspan="2">wichtig</td></tr>
<tr><td>Betreiber von Internet-Knoten</td><td rowspan="4">wichtig</td><td></td></tr>
<tr><td>Anbieter von Cloud-Computing-Diensten</td><td></td></tr>
<tr><td>Anbieter von Rechenzentrumsdiensten</td><td></td></tr>
<tr><td>Betreiber von Content Delivery Networks (CDN)</td><td></td></tr>
</table>

Tabelle 1: Übersicht NIS2 betroffene Organisationen

Teil III Ergebnisdarstellung

Die Branchenrisikoanalyse setzt sich das Ziel, möglichst umfassend alle Gefahren, die sich für TELKOs und ISPs ergeben, zu identifizieren.

In den Vorversionen bis zur Version 3.0-2020 der Risikoanalyse wurden mehrere allgemeine Gefahrenmodelle erarbeitet und für die Risikoidentifikation herangezogen. Parallel dazu wurden die Gefahren durch die Einführung der 5G-Technik basierend auf den normativen Vorgaben zusammengestellt und entsprechend berücksichtigt. In Summe liegen der Risikoanalyse 526 aggregierte Gefahren zugrunde, die in weiterer Folge in der bereits beschriebenen Methode zu Risiken bewertet wurden. Die Gefahrenkataloge sind in den Anhängen zusammengestellt. Dort findet man auch eine Kurzbeschreibung der definierten übergeordneten Gefahrenfelder.

5. Risikobewertungskriterien; Grundlage der Risikobewertung

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

5.1 Allgemeines zur Herleitung der Bewertungskriterien

Die Bewertungskriterien wurden im Rahmen des Updatezyklus evaluiert. Sie bleiben im Vergleich zur Version 3.0 unverändert, da sie nach wie vor eine sinnvolle Abstufung von Risiken zueinander erlaubt. An dieser Stelle sei darauf hingewiesen, dass die vorliegende Risikobetrachtung primär auf die Relationen von Risiken zueinander abzielt.

Den Ergebnissen liegt primär die Expertise der Teilnehmenden zugrunde und KEINE empirisch erhobenen Daten zu Ereignissen oder technisch gemessenen Ausfallszeiten.

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 weiter wichtig darzustellen, dass es einer skalierbaren und damit einer für alle TELKO und ISP gleichgewichteten Abstufung bedarf, damit die Risiken in Relation für alle Organisationsgrößen gleichverteilt sind.

Analog zum Bild der Sicherheitskette, wo immer das schwächste Glied die gesamte Stärke der Kette determiniert, wurde eine Bewertungsmetrik festgelegt bzw. wieder evaluiert, die von ganz kleinen Organisationen bis hin zu großen bis sehr großen TELKOs und ISPs sinnvoll eingesetzt werden kann.

5.2 Festlegung Eintrittswahrscheinlichkeiten und Machbarkeit

5.2.1 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 2: Bewertung der Eintrittswahrscheinlichkeit bei techn. und Naturgefahren

5.2.2 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 / Expert*innen-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 Fach-kenntnisse werden vorausgesetzt z. B. APTs - auch in Kombination mit social Engineering	2

Machbarkeit Intentionale Gefahren			Bewertung Punkte
Eintritts-wahrscheinlichkeit	Verbale Beschreibung	Aufwand in Zeit und Know-how	
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 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.

5.3 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. Wieder-herstellungsaufwand 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 + 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, Kapitalmaßnah-men durch den jur. Eigentümer erforderlich	**4**
katastrophal	Ereignis betrifft >1920%h aller Kunden. Notrufe/Notrufträger flächendeckend betroffen/ verfügbarkeitskritische Services betroffen. Performanceeinbußen bei Teilen des Netzes/Services/ Applikationen sind so hoch, dass diese de facto nicht genutzt werden können	(wie hoch + 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, Kapitalmaßnah-men 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 4: Bewertung der Schadensdimension

5.4 Risikobewertungsprozess – Übersicht

Die in der Version 3.0-2020 identifizierten 131 Einzelrisiken wurden in einem ersten Schritt evaluiert. Im Ergebnis wurden 113 Einzelrisiken neu bzw. angepasst zusammengestellt.

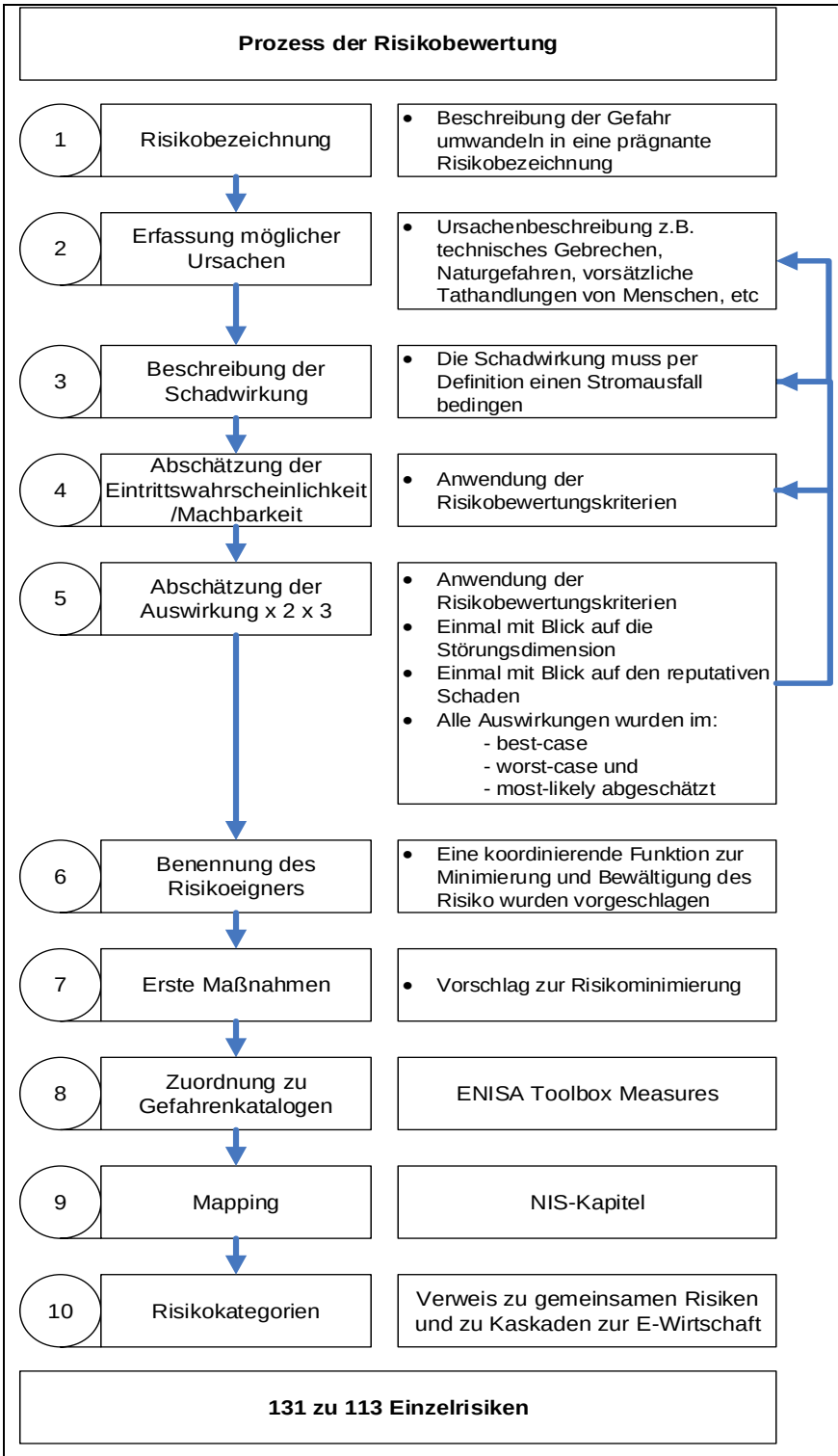

Abbildung 5: Risikobewertungsprozess

In Summe wurden in der nebenstehenden Systematik **113** Risiken erfasst.

Diese wurden in 5 Arbeitsworkshops zu je 4-5h durchgeführt.

Dabei wurden 3 neue Risiken identifiziert und hinzugefügt.

6. Ergebnisdarstellung der Einzelrisiken

6.1 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 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
ISPs	0	0	0	Einheitlichen Einbautenkataster anstreben, ggfs. Beauskunftung empfehlen, Wegeredundanz	I-04, TBX-TM11	Technik und Infrastruktur

Tabelle 6: Teil 2 der Einzelrisikoerfassungstabelle

Fortsetzung der Tabelle

P	Q	R
Gültigkeit bis	NIS-MAP	Kaskaden, gem. Risken
11.03.26	7	G, K

Tabelle 7: Teil 3 der Einzelrisikoerfassungstabelle

- Spalte A, laufenden 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 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 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 anzustreben, 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 der Risikokategorie Technik und Infrastruktur.
- Spalte P definiert eine Gültigkeitsdauer dieses Risikos. Dies wird durch den festgelegten Review Zyklus 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 vermerkt, ob es sich hier um ein mit der Energiewirtschaft „gemeinsames“ Risiko(G) oder um ein Risiko mit Kaskadenpotential handelt (K).

Die Risikobewertungen wurden immer in einem Best Case im Worst Case und im Most Likely Fall bewertet. Dabei wurden immer alle Risiken auf **einer** Risikomatrix zusammengestellt.

7. Ergebnisdarstellung der Aggregationsrisiken

7.1 Aggregationsprozess

Basierend auf den Ergebnissen der Risikobewertung aus Version 3.0-2020 mit 131 Einzelrisiken wurden 113 Einzelrisiken neu bewertet. Es wurden 21 Risiken aus der Version 3.0-2020 gelöscht und drei Einzelrisiken hinzugefügt.

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 Aggregationsvorschlag zu erarbeiten. Die Aggregationsrisiken wurden anschließend in einem iterativen Prozess zusätzlich 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.

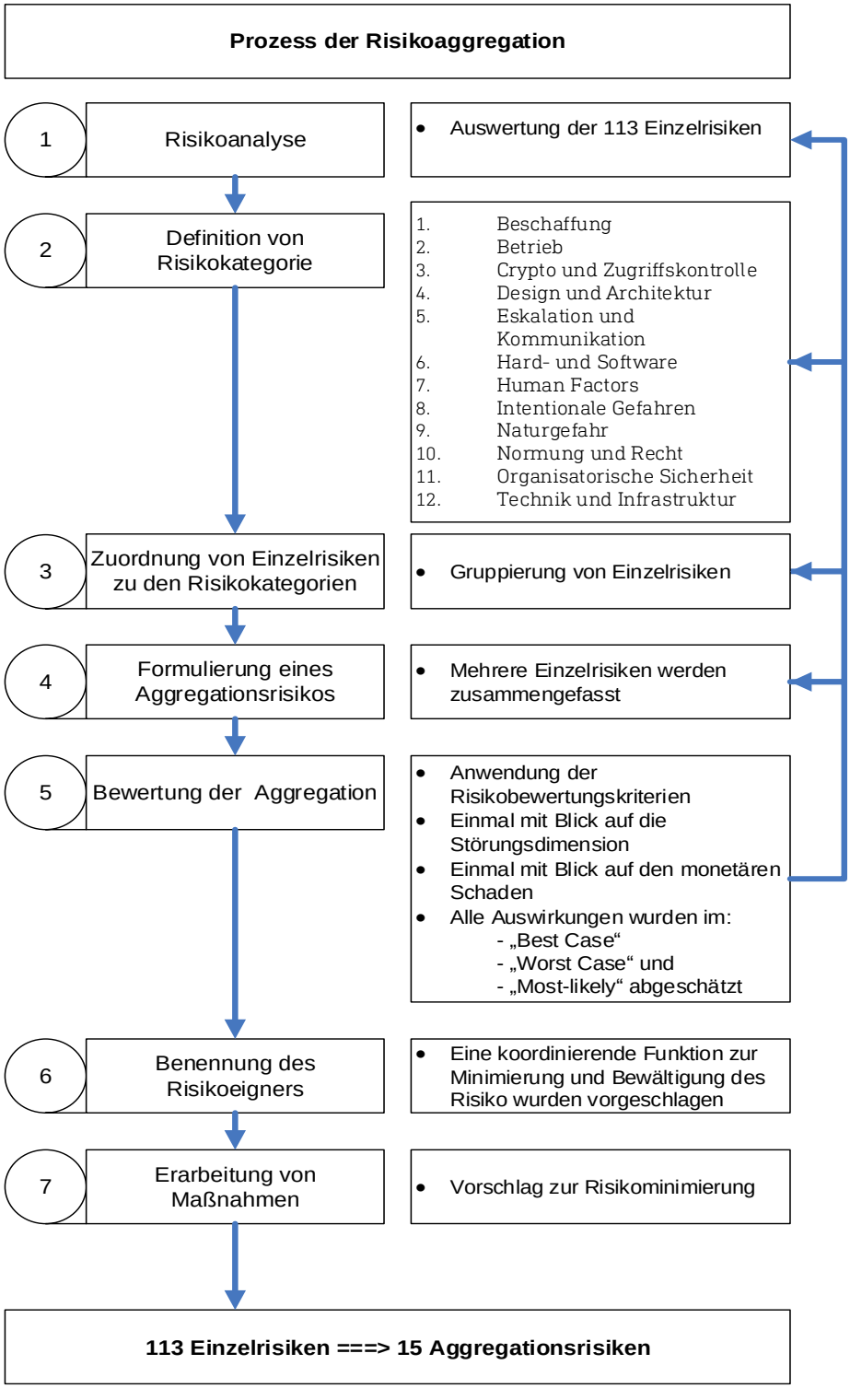

Abbildung 6: Risikoaggregationsprozess

7.2 Aggregationsrisikomatrix im „Worst Case“

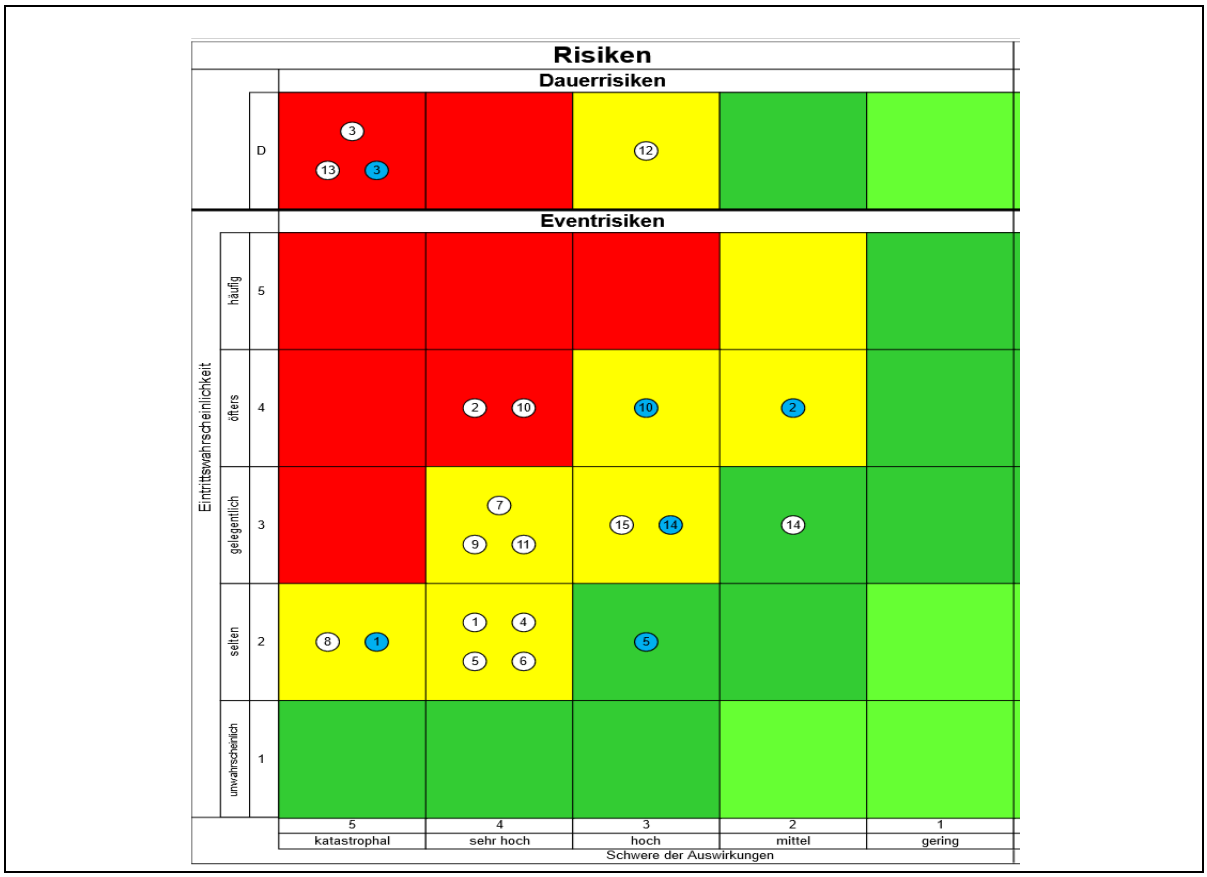

Abbildung 7: Aggregationsmatrix im "Worst Case" -2023

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

Eine Kurzbeschreibung der Aggregationsrisiken ist im Kapitel 7.5 zusammengestellt. Eine eingehendere Diskussion der Aggregationsrisiken ist im Abschnitt 8, Detailauswertung der Aggregationsrisiken aufbereitet.

7.3 Aggregationsrisikomatrix im „Most-Likely“

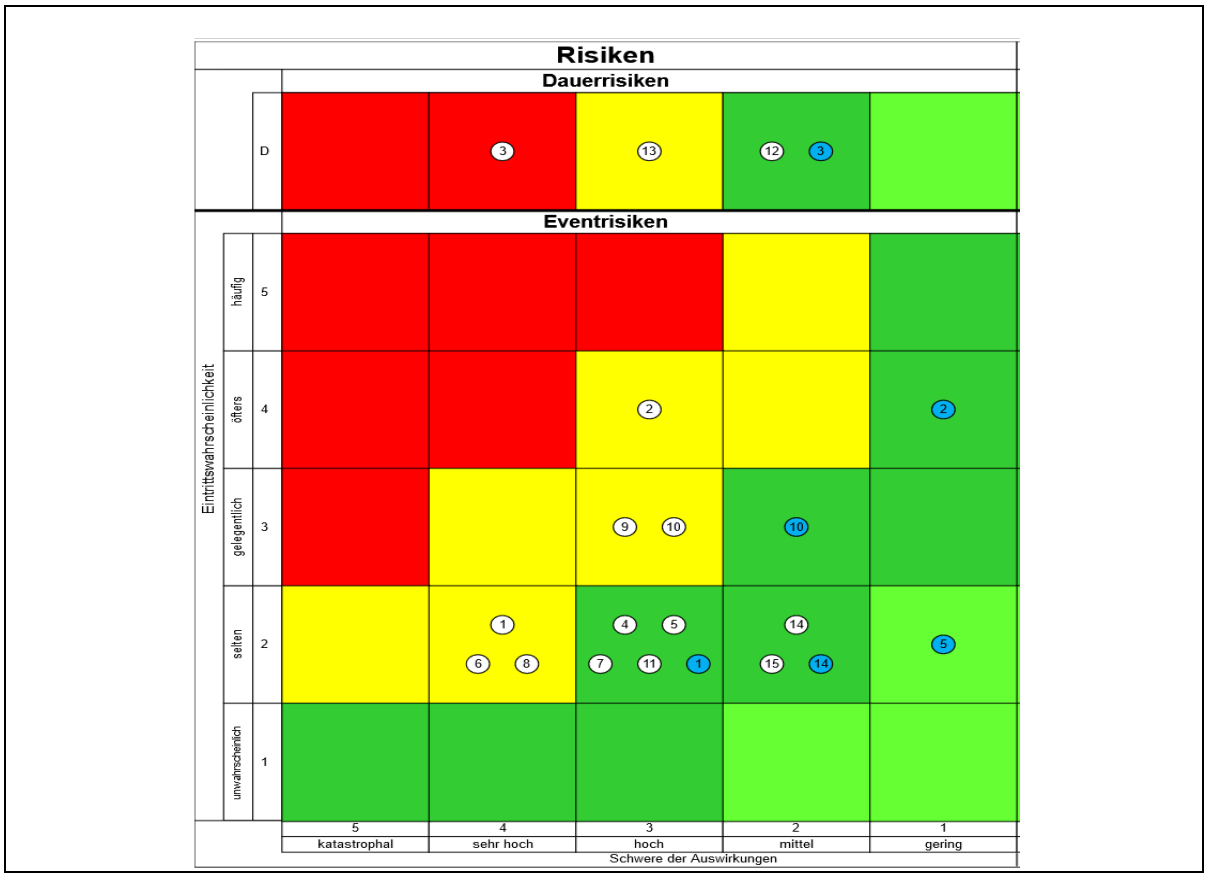

Abbildung 8: Aggregationsmatrix im "Most-likely"-2023

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

Eine Kurzbeschreibung der Aggregationsrisiken ist im Kapitel 7.5 zusammengestellt. Eine eingehendere Diskussion der Aggregationsrisiken ist im Abschnitt 8, Detailauswertung der Aggregationsrisiken aufbereitet.

7.4 Aggregationsrisikomatrix im „Best Case“

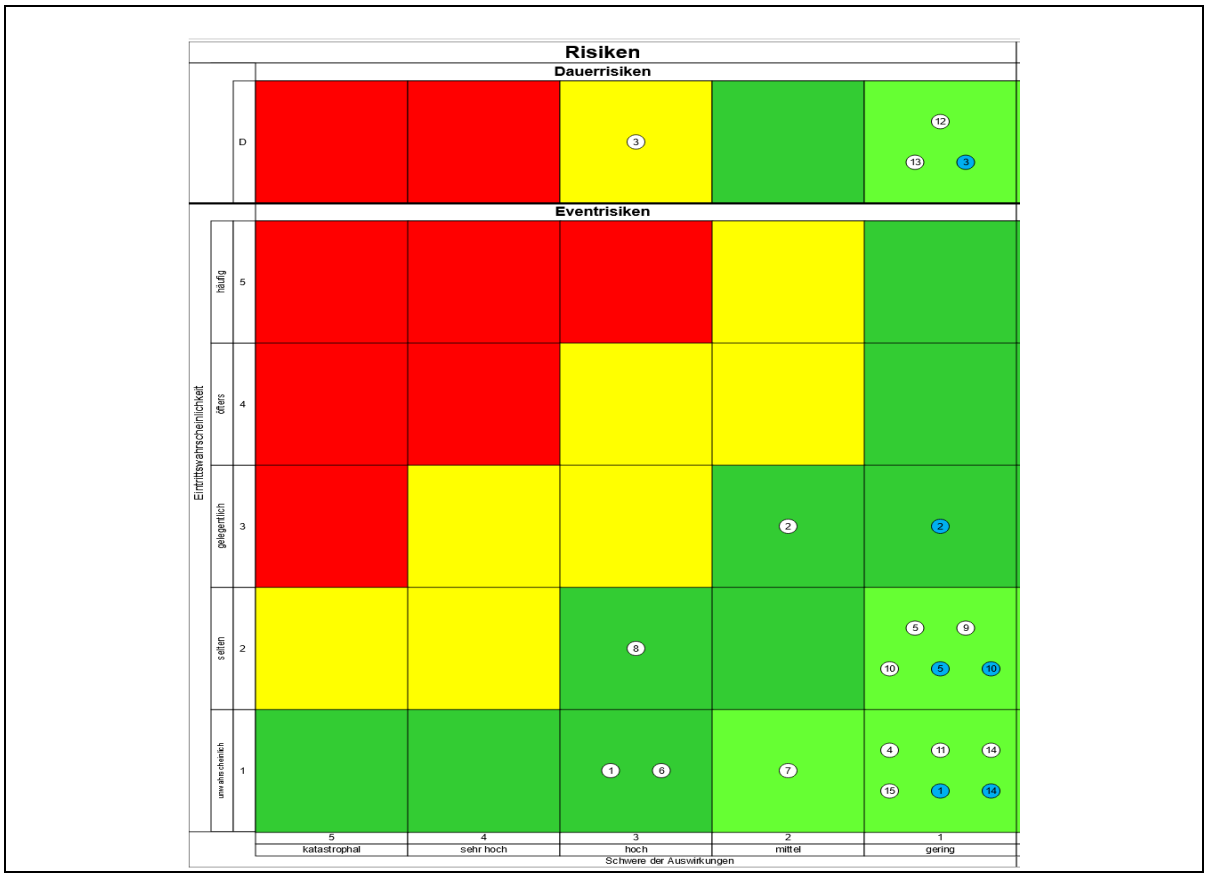

Abbildung 9: Aggregationsmatrix im "Best Case"-2023

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

Eine Kurzbeschreibung der Aggregationsrisiken ist im Kapitel 7.5 zusammengestellt. Eine eingehendere Diskussion der Aggregationsrisiken ist im Abschnitt 8, Detailauswertung der Aggregationsrisiken aufbereitet.

7.5 Beschreibung der Aggregationsrisiken

Nr	Risikobezeichnung	Ursache	Wirkung	Risiko-Owner	Maßnahmen zur Risikobewältigung	Anmerkungen; Maßnahmenvorschläge
1	Ausfall wesentlicher Infrastrukturen oder Betriebsmittel	Naturgefahren, Technische Gefahren	Ausfall von wesentlichen Dienstleistungen bis zu 1920%h	TELKO/ISP	Risikomanagement der Infrastrukturen durchführen. Planung und Tests von Redundanzen. Monitoring der Servicequalität, Notfallpläne erarbeiten und Ablaufpläne testen.	TBX-TM-11, TM06, SM06, SA07
2	Gefahr der Beschädigung oder Zerstörung oder Diebstahl wichtiger physischer Betriebsmittel	Fahrlässigkeit und vorsätzliche Handlungen durch Personen	Erhebliche Störungen von 2 bis 1920%h	TELKO/ISPs	Entsprechender Objektschutz und Vorratshaltung von sicherheitsrelevanten Ersatzsystemen	TBX-TM06, SM06,
3	Kriminelle Handlungen aus dem Cyberraum sowie Cyber-Fraud	Heterogene Motivationslage z. B. Sabotage, Industriespionage und monetäre Absichten und/oder politische Absichten, Betrug	Hoher Imageschaden, Zerstörung von IKT-Infrastruktur-Ausfall > 1920%h, damit verbundener monetärer Schaden, Abgriff schützenswerter Informationen	TELKO/ISP	Enge Zusammenarbeit mit CSIRT, Behörden und Betroffenen und ggfs. mit anderen Betreibern. Sicherheitslagebild, freiwilliges Incident Sharing	TBX-TM11, SA09
4	Mögliche, erhebliche Defizite bei IKT-Design und Systemarchitektur	Mögliche Planungsfehler, fehlendes Monitoring, unerwartete Bandbreiten-entwicklung, Fehlconfig., technische Fehler, unterlassenen Sicherheits-maßnahmen	Ausfall von kritischen Services für bis zu 12 h oder mehr	TELKO/ISP	Design und Implementation Reviews unter Mitwirkung von Expert*innen im Rahmen des Life-Cycle sicherstellen.	TBX-TM01, TM02, TM04, TM09, TM10, SA03, SA04,

Nr	Risikobezeichnung	Ursache	Wirkung	Risiko-Owner	Maßnahmen zur Risikobewältigung	Anmerkungen; Maßnahmenvorschläge
5	Negative Auswirkungen von politisch/rechtlichen Vorgaben aufgrund sich ändernden Rahmen-bedingungen auch öffentliche Wahrnehmung	Spannungsverhältnis zwischen staatlichen und wirtschaftlichen Interessen	Erhöhte Kosten und Nichteinführung von Technologien, Nachteile im internationalen Wettbewerb (EU). ggfs. Kontraindika-tionen zur IKT-sicherheit.	TELKO	Einbindung der betroffenen Branche zwecks Einholung sachlicher Vorschläge zum Ausgleich zwischen staatlichen und wirtschaftlichen Interessen	TBX-SM06, SM07, SM08,
6	Unzureichende Berücksichtigung von ISMS-Anforderungen im Beschaffungsprozess	Kostendruck, mangelnde Einbindung von ISB-Security in den Prozess, mangelnde Awareness der Hersteller/Lieferanten	Potenzieller Mehraufwand bei der nachträglichen Absicherung (betrieblich/monetär)	TELKO/ISP	Geeignete Sicherheits-anforderungen in jeder IKT-relevanten Ausschreibung/ Beschaffung berücksichtigen, z.B. EU-Mindestsicherheitsstandards anführen	TBX-TM08, SM03, SM04
7	Mangelhaftes Notfall-, Krisen- und Kontinuitäts-management	Mögliche wenige Identifikation der obersten Leitung und damit verbundene Kosten, mangelnde Priorität, Unverständnis für die Notwendigkeit bei den Mitarbeitern	Mögliche erhebliche Verlängerung der Bearbeitung von Sicherheitsangelegenheiten /-Vorfällen bei Vertraulichkeit, Verfügbarkeit und Integrität	TELKO/ISP	Bewusstseinsbildung bei der obersten Leitung, Awareness-maßnahmen bei den Mitarbeitern, Lessons Identified und Lessons Learned Prozess aufsetzen (PDCA Kreislauf durchlaufen) An einschlägigen Übungen teilnehmen. Qualifiziertes Personal einsetzen.	TBX-TM11, SA09
8	Erhebliche Probleme beim Patch- und Update-Prozess	Mangelnde Tests, nicht alles lässt sich in den Teststellungen testen, mangelnde Verfügbarkeit von Testumgebungen / mögliche Defizite im Changemanagement-prozess	Erhebliche/r Einschränkungen und/oder Wiederherstellungsaufwand bei Services für einen Zeitraum von max. 1920 %h z. B. Abrechnungsdatenbank	TELKO/ISP	Trennung von Security- und funktionalen Patches inkl. Relevanz- und Impactüber-prüfungen und ggfs. Test-stellungen im Einzelfall. Roll-out-Planung inkl. Fall-back-Szenarien erarbeiten.	TBX-TM-07, TBX-SA-02, SA-01

Nr	Risikobezeichnung	Ursache	Wirkung	Risiko-Owner	Maßnahmen zur Risikobewältigung	Anmerkungen; Maßnahmenvorschläge
9	Defizite bei Identity and user access control (IAM)	Mangelnde Sensibilisierung von MA / Rechtevergabe / fehlendes Know-how / fehlende Ressourcen / technische Limitierungen	Mögliche erhebliche Einschränkungen bei Verfügbarkeit, Integrität, Vertraulichkeit; hoher Imageschaden	TELKO/ISP	Sensibilisierung im Management, Segregation of Duties, Automatisierungen im User Management inkl. regelmäßige Reviews der Berechtigungen.	TBX-TM-01, TM-03, SA-01
10	Verlust der Vertraulichkeit von geschützter Information	Mangelnde Information Security und oder unsichere Crypto	Möglicher erheblicher Imageschaden, mögliche Strafen, möglicher Vertraulichkeits-/ Integritätsverlust, Haftungsübernahmen, Geschäftsverlust	TELKO/ISP	Entsprechendes Management der Informationssicherheit einführen ISO 27k, CIS TOP20 implementieren, und ggfs. Sicherheitsüberprüfungen von Personen durchführen lassen	TBX-TM-01, TM-02, SA-01
11	Ausfall oder erhebliche Serviceeinschränkungen bei singulären IKT-Lieferanten oder Hersteller	Abhängigkeit von singulären Lieferanten, Einstellung der Geschäftstätigkeit eines Lieferanten	Erhebliche Verzögerungen bei Wiederherstellung von Betriebseinschränkungen	TELKO/ISP	Grundsätzliche Vermeidung von singulären Abhängigkeiten, z.B. eine zwei Vendor Strategie evaluieren	TBX-TM-01, SM-05 Klarstellung, Multi-Vendor; Möglichkeit des Einsatzes unterschiedlicher Komponenten unterschiedlicher Hersteller
12	Mängel in der Betriebsführung	Zeit- und Kostendruck, Personalengpässe, strategische Fehlsteuerung	Vernachlässigung der Security Hygiene, Nichteinhaltung von Standards, Imageschaden, Verfügbarkeitsprobleme, Mehraufwand zur Absicherung der Systeme	TELKO/ISP	Ausreichende Berücksichtigung von Betriebsführungsrisiken im Risikomanagement des Unternehmens. Betriebshandbuch aktuell halten.	TBX-TM01-09, TM11, TM-04, SA06, SA07, SA09

Nr	Risikobezeichnung	Ursache	Wirkung	Risiko-Owner	Maßnahmen zur Risikobewältigung	Anmerkungen; Maßnahmenvorschläge
13	Vulnerabilities bei Hard- und Software	Gefahr der fehlenden Security Awareness bei Herstellern und Lieferanten, organisatorische Defizite	Mögliche erhebliche betriebliche Einschränkungen bei Ausnutzung und/oder bei Bekanntwerden, Integritäts- und Vertraulichkeitsverlust und Kundenendgeräte stellen hohen Multiplikationsfaktor für betriebliche Einschränkungen dar	TELKO/ISP	Lieferanten/Hersteller zur rechtzeitigen und angemessenen Reaktion auf bekanntgewordene Schwachstellen verpflichten. Gesetzliche Haftungen von Lieferanten für vulnerable Produkte	TBX-TM-01-05, TM-07-TM10, SA01-02, SA05
14	Mangelnde Compliance (Datenschutz, Standards, Verträge etc.) oder fehlende Legistik	Zertifizierung fehlt/ fehlende Standards, mangelnde Implementierung in der Organisation	Mögliche Verletzung der SLAs, damit verbunden Pönale, mögliche Datenschutzverletzungen	TELKO/ISP	Innerbetriebliche Meldestelle für vermutete Compliance-verletzungen institutionalisieren inkl. Revisionsprozess. Aus- und Fortbildungsmaßnahmen	TBX-TM-09-10, SA-05,
15	Ausfall der übergeordneten Stromversorgung (Energiemangellage)	flächendeckenden Stromausfall oder sonstige wesentliche techn. Gebrechen für > mind. 30min.	Ausfälle von Services/Dienstleistungen für ca. 360 %h	TELKO/ISP	USV-Zeiten und Notstromversorgung sowie Anschlussversorgung sicherstellen und entsprechende BCM-Pläne vorhalten und beüben	TBX-TM-11, EFF6

Tabelle 8: Kurzbeschreibung der Aggregationsrisiken

8. Detailauswertung der Aggregationsrisiken

Die Detailauswertung der Aggregationsrisiken erfolgt unter einem „Worst-Case“ Aspekt. Die nachfolgenden Bewertungen beziehen sich daher auf diese Sichtweise. Die Diskussion der Eingruppierung erfolgt auf Basis der betrieblichen Risikobetrachtung und nicht auf Basis der monetären Bewertungen.

8.1 Übersicht der hohen Aggregations- und Dauerrisiken

Nr	Risikobezeichnung	Ursache	Wirkung
2	Gefahr der Beschädigung oder Zerstörung oder Diebstahl wichtiger physischer Betriebs-mittel	Fahrlässigkeit und vorsätzliche Handlungen durch Personen	Erhebliche Störungen von 2 bis 1920 % h
3	Kriminelle Handlungen aus dem Cyberraum sowie Cyber-Fraud	Heterogene Motivationslage z. B. Sabotage, Industriespionage und monetäre Absichten und/oder politische Absichten, Betrug	Hoher Imageschaden, Zerstörung von IKT-Infrastruktur-Ausfall > 1920%h, damit verbundener monetärer Schaden, Abgriff schützenswerter Informationen
10	Verlust der Vertraulichkeit von geschützter Information	Mangelnde Information Security und oder unsichere Crypto	Möglicher erheblicher Imageschaden, mögliche Strafen, möglicher Vertraulichkeits-/Integritätsverlust, Haftungsübernahmen, Geschäftsverlust
13	Vulnerabilities bei Hard- und Software	Gefahr der fehlenden Security Awareness bei Herstellern und Lieferanten, organisatorische Defizite	Mögliche erhebliche betriebliche Einschränkungen bei Ausnutzung und/oder bei Bekanntwerden, Integritäts- und Vertraulichkeitsverlust und Kundenendgeräte stellen hohen Multiplikationsfaktor für betriebliche Einschränkungen dar

Tabelle 9: Hohe Einzel- und Dauerrisiken; hellrote Risken sind Dauerrisiken

8.1.1 RISIKO NR. 2, GEFAHR DER BESCHÄDIGUNG ODER ZERSTÖRUNG ODER DIEBSTAHL WICHTIGER PHYSISCHER BETRIEBSMITTEL

Aggregation: Dieses Risiko setzt sich aus den 7 Einzelrisiken zusammen.

Risikotyp: Eventrisiko

Zusammenfassung: Dieses Risiko fasst de facto drei wesentliche Aspekte betrieblicher Verfügbarkeitsaspekte zusammen. Einmal ungewollte, aber leider sehr häufig vorkommende Manipulationen im Boden und damit verbunden Unterbrechungen bei 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 in der unmittelbaren Nähe zu Großveranstaltungen mit entsprechendem Potential zu Vandalismus. Zwischen dem Aggregationsrisiko 3 und 2 wurde eine klarere Trennung von physischen Bedrohungen und kriminellen Handlungen aus dem Cyberraum vorgenommen.

Mögliche wesentliche Schadwirkungen: Erhebliche Einschränkungen bei Verfügbarkeiten bzw. sehr hoher Wiederherstellungsaufwand auch determiniert durch das Vorhalten von Redundanzen.

Unmittelbar zugeordnete Empfehlungen: Aus dem Aggregationsrisiko 2 lassen sich folgende Empfehlungen ableiten:

- Durch proaktive Informationspolitik sollen Betriebsunterbrechungen durch „Baggerangriffe" möglichst minimiert werden.
- Entsprechend ausgeprägter Objektschutz, der einen risikogetriebenen Ansatz verfolgt und keine Standards vorgibt. Hier wird stellvertretend z. B. die ÖNORM S2420 angeführt.
- Ein entsprechend angepasstes BCM, dass die Wiederanlaufzeiten auf Basis einer Business Impact Analyse berücksichtigt

8.1.2 RISIKO NR. 3, KRIMINELLE HANDLUNGEN AUS DEM CYBERRAUM SOWIE CYBER-FRAUD

Aggregation: Dieses Risiko setzt sich aus den 14 zusammen.

Risikotyp: Dauerrisiko

Zusammenfassung: Dieses Risiko wurde von einem Eventrisiko zu einem Dauerrisiko hochgestuft. Es ist dies den Erkenntnissen der letzten drei Jahre geschuldet, da die kriminellen Handlungen aus dem Cyberraum an Intensität, Variabilität und an „Qualität" deutlich zugenommen haben. Es umfasst daher mehrere Aspekte, die wie folgt beschrieben werden können:

- Gezielter Missbrauch im großen Stil von Leistungsmerkmalen von TK-Anlagen mit dem Ziel monetärer Vorteilsnahme
- Abhören von Leitungen
- Missbrauch von Wartungszugängen - out of band Management.
- Traffic-Schleuder des Kunden
- Provisionierung von Kryptographie (SIM-Karten) - Verlust von Vertraulichkeit und Integrität von Schlüssel
- Angriffe durch potentielle kriminelle Organisationen/Vereinigungen mit dem Ziel monetärer Vorteilsnahme (Cybercrime)
- "Identitätsklau" - Betrug
- Missbrauch von Routingprotokollen (inkl. DNS, SS7, BGP, etc.)
- Adressspoofing von Internetadressen
- Absichtliche Backdoors und/oder undokumentierte, unerwartbare und schwer prüfbare Funktionen mit Datenabfluss bei Core-Komponenten
- Kompromittierte Endkundengeräte werden als "Jump-Server" von Cyberkriminellen missbraucht

- Gefahr von Downgrade-Attacken aller Art (TLS, Rückfall auf 3G, 2G etc.)
- Gefahr des Betriebs einer nicht autorisierten Basisstation
- Rufnummernspoofing

Mögliche wesentliche Schadwirkungen: Kriminelle Handlungen haben im Wesentlichen das Ziel der monetären Vorteilsnahme, unabhängig davon, ob der Netz- und/oder Servicebetreiber selbst Opfer der kriminellen Handlungen ist. Solche Angriffe sind in der Regel mit einem hohen Imageschaden verbunden. Parallel können IKT-Infrastrukturen für einen längeren Zeitraum ausfallen. Damit verbunden sind hohe monetäre Schäden die auch durch gesetzliche Auflagen zusätzlich verstärkt werden (Strafzahlungen).

Unmittelbar zugeordnete Empfehlungen: Aus den Einzelrisiken zu Aggregationsrisiko 3 lassen sich folgende Empfehlungen ableiten:

- Enge Zusammenarbeit mit CSIRT, Behörden und Betroffenen und ggfs. mit anderen Betreibern. Sicherheitslagebild, freiwilliges Incident Sharing, Intensivierung des Informationsaustausches „Sicherheitslagebild und Incident Sharing“
- Implementierung von Fraud-Detection-Systemen
- Gezielter Einsatz und Unterstützung von Netzwerkverschlüsselung, klare Empfehlung für end-to-end-Verschlüsselung;
- Regulative Vorgaben schaffen zur Überbindung an die Hersteller / Optimierung des Provisionierungsprozesses
- Prüfen des Rechts (noch) nicht betroffener Unternehmen / Organisationen zum frühzeitigen Ergreifen präventiver Maßnahmen gegen (D)DOS
- Intensivierung von Mitarbeiterschulungen inkl. der Erarbeitung und Implementierung von Responseplans für bereits bekannte Cyberattacken
- Awareness bei Endkunden schaffen, regelmäßige Empfehlung zur Cyber Hygiene
- entsprechende BCM-Pläne entwickeln, end-to-end Verschlüsselung auf Applikationsebene promoten
- Änderungen an rechtlichen Rahmenbedingungen anstreben, dies gilt insbesondere bei den aktuellen Rufnummernspoofing Angriffen

8.1.3 RISIKO NR. 10, VERTRAULICHKEITSVERLUST VON GESCHÜTZTEN INFORMATIONEN

Aggregation: Dieses Risiko setzt sich aus 7 Einzelrisiken zusammen.

Risikotyp: Eventrisiko

Zusammenfassung: Dieses Risiko adressiert die Komplexität, kryptographische Methoden effektiv zu implementieren und deren Wirksamkeit über den gesamten Life-Cycle hinweg auch „nachzuweisen“. Durch die Aggregation der angeführten Einzelrisiken soll auch

verdeutlicht werden, dass ein Informationssicherheitsmanagementsystem den gesamten Life-Cycle und alle Stakeholder der Informationssicherheit miteinschließen muss.

Mögliche wesentliche Schadwirkungen: Erheblicher Imageschaden sowie Strafen, bis hin zu hohen Geschäftsverlusten

Unmittelbar zugeordnete Empfehlungen: Aus dem Aggregationsrisiko 10 lassen sich folgende Empfehlungen ableiten:

- Es wurde in den Einzelrisiken viele Aspekte empfohlen, die in ein umfassendes Sicherheitsmanagement System münden. Mit Blick auf NISG/NISV sind dies keine Empfehlungen mehr, sondern rechtliche Anforderungen.
- Ständige Aus- und Fortbildung der Mitarbeiter inklusive dem Top-Management
- Implementierung der CIS-Top 20 bzw. Umsetzung der Controls der ISO 27.002 oder vergleichbarer Empfehlungen
- Mitarbeiterschulungen, Responseplans, automatisierte Verhaltenskontrolle, Monitoring und Logging intensivieren; enge Zusammenarbeit mit Behörden und Betroffenen, Sicherheitslagebild, ausreichende Ressourcen
- In diesem Kontext muss darauf verwiesen werden, dass die Branche nach wie vor empfiehlt, Verschlüsselung nicht durch gesetzliche Auflagen aufzuweichen.

8.1.4 RISIKO NR. 13, VULNERABILITIES BEI HARD- UND SOFTWARE

Aggregation: Dieses Risiko setzt sich aus den 7 Einzelrisiken zusammen.

Risikotyp: Dauerrisiko

Zusammenfassung: Das Risiko Nr. 13 beschäftigt sich mit den ständigen Schwachstellen bei Hard- und Software, die in weiterer Folge intentional ausgenützt werden.

Stellvertretend für APTs Advanced Persistent Threats werden hardwarenahe Schwachstellen angesprochen, die insbesondere hardwarenahe Sicherheitsmechanismen aushebeln sollen. Man geht davon aus, dass die Attraktivität von solchen Schwachstellen insbesondere bei der Kompromittierung von VM-Umgebungen hoch erscheint, da der Trend zur Virtualisierung ungebrochen ist. Mit solchen Vulnerabilitäten kann man die Vertraulichkeit erheblich erschüttern. Neben den APTs stehen Schwachstellen bei Hard- und Software insbesondere bei CPEs mit im Fokus der Betrachtungen, die zu einer hohen Risikobewertung geführt haben. Parallel dazu sind Vulnerabilitäten bei Legacy Systemen, die aus vielerlei Gründen erheblich länger eingesetzt werden (müssen) mit ein Beweggrund, hier ein hohes Risiko ex ante darzustellen.

Mögliche wesentliche Schadwirkungen: Erhebliche betriebliche Einschränkungen bei Ausnutzung und/oder bei Bekanntwerden von Schwachstellen. Zusätzlich stellen Integritäts- und Vertraulichkeitsverluste (auch bei Kundenendgeräte) einen hohen Multiplikationsfaktor für betriebliche Einschränkungen dar.

Unmittelbar zugeordnete Empfehlungen: Aus dem Aggregationsrisiko 13 lassen sich folgende Empfehlungen ableiten:

- Da es sich hier zum Teil um APTs handelt, müssen auf der europäischen Ebene die Anstrengungen intensiviert werden, entsprechende Testumgebungen, Testregimes und Testfacilities zu schaffen, die in weiterer Folge ein IKT-CE-Kennzeichnung erlauben
- Die Hersteller werden angehalten, entsprechende V-Modelle bei der Entwicklung von Hard- und Software einzuführen und zu veröffentlichen (vgl. dazu die Vorgaben der DIN / ISO 61508ff)
- Intensivierung des Informationsaustauschs zwischen Betreibern und CSIRTs bzgl. erkannter Schwachstellen bei Hard- und Software
- Im Beschaffungsprozess soll eine Hinweispflicht seitens der Lieferanten und Hersteller verankert werden, dass auf bekannt gewordene Schwachstellen proaktiv hinzuweisen und ggfs. Workarounds anzubieten (speziell bei CPEs) ist.
- Lieferanten/Hersteller zur rechtzeitigen und angemessenen Reaktion auf bekanntgewordene Schwachstellen verpflichten; gesetzliche Haftungen von Lieferanten für vulnerable Produkte
- Hersteller/Lieferanten zur Zertifizierung verpflichten; harmonisiertes/robustes Patchmanagement, wird mit NIS2 und durch CRA mitigiert. Tests, Rolloutplanung, Fall-Back-Planung, Lieferanten und Hersteller zur Mitigation bei Schwachstellen vertraglich verpflichten
- Qualitätskontrolle bei CPEs, Procurement, Lifecycle Betrachtung, Angriffs- und Anomalieerkennung, Sicherheitszertifikate für neu eingeführte CPEs bei Inverkehrbringung. Bessere Spezifikationen, bessere Verträge mit Lieferanten, besonderes Augenmerk beim Beschaffungsprozess
- Entsprechende Verträge mit Lieferanten/Hinweispflicht auf erkannte Lücken seitens der Hersteller/Lieferanten, Nutzung und Einbeziehung von CSIRTs, Lieferanten und Hersteller zur Mitigation bei Schwachstellen vertraglich verpflichten
- Regulatorische Vorgaben/Einschränkungen, EU-weite Tests initiieren
- Möglichkeit von Betreibersperren vorsehen, rechtliche Grundlagen für Monitoring-möglichkeiten schaffen
- Awareness bei den Kunden schaffen; Kundenschutz mittels Aufklärung durch Konsumentenschutzvertretungen

8.2 Übersicht der mittleren Aggregations- und Dauerrisiken

Nr	Risikobezeichnung	Ursache	Wirkung
1	Ausfall wesentlicher Infrastrukturen oder Betriebsmittel	Naturgefahren, Technische Gefahren	Ausfall von wesentlichen Dienstleistungen bis zu 1920%h
4	Mögliche, erhebliche Defizite bei IKT-Design und Systemarchitektur	Mögliche Planungsfehler, fehlendes Monitoring, unerwartete Bandbreitenentwicklung, Fehlconfig., technische Fehler, unterlassenen Sicherheitsmassnahmen	Ausfall von kritischen Services für bis zu 12 h oder mehr
5	Negative Auswirkungen von politisch/rechtlichen Vorgaben aufgrund sich ändernden Rahmenbedingungen auch öffentlicher Wahrnehmung	Spannungsverhältnis zwischen staatlichen und wirtschaftlichen Interessen	Erhöhte Kosten und Nichteinführung von Technologien, Nachteile im internationalen Wettbewerb (EU). ggfs. Kontra-indikationen zur IKT-Sicherheit.
6	Unzureichende Berücksichtigung von ISMS-Anforderungen im Beschaffungsprozess	Kostendruck, mangelnde Einbindung von ISB-Security in den Prozess, mangelnde Awareness der Hersteller/Lieferanten	Potenzieller Mehraufwand bei der nachträglichen Absicherung (betrieblich/monetär)
7	Mangelhaftes Notfall-, Krisen- und Kontinuitätsmanagement	Mögliche wenige Identifikation der obersten Leitung und damit verbundene Kosten, mangelnde Priorität, Unverständnis für die Notwendigkeit bei den Mitarbeitern	Mögliche erhebliche Verlängerung der Bearbeitung von Sicherheitsangelegenheiten/-Vorfällen bei Vertraulichkeit, Verfügbarkeit und Integrität
8	Erhebliche Probleme beim Patch- und Update-Prozess	Mangelnde Tests, nicht alles lässt sich in den Teststellungen testen, mangelnde Verfügbarkeit von Testumgebungen / mögliche Defizite im Changemanagement-prozess	Erhebliche/r Einschränkungen und/oder Wiederherstellungsaufwand bei Services für einen Zeitraum von maximal 1920 %h z. B. Abrechnungsdatenbank
9	Defizite bei Identity and user access control (IAM)	Mangelnde Sensibilisierung von MA / Rechtevergabe / fehlendes Know-how / fehlende Ressourcen / technische Limitierungen	Mögliche erhebliche Einschränkungen bei Verfügbarkeit, Integrität, Vertraulichkeit; hoher Imageschaden
11	Ausfall oder erhebliche Serviceeinschränkungen bei singulären IKT-Lieferanten oder Hersteller	Abhängigkeit von singulären Lieferanten, Einstellung der Geschäftstätigkeit eines Lieferanten	Erhebliche Verzögerungen bei Wiederherstellung von Betriebseinschränkungen
12	Mängel in der Betriebsführung	Zeit- und Kostendruck, Personalengpässe, strategische Fehlsteuerung	Vernachlässigung der Security Hygiene, Nichteinhaltung von Standards, Imageschaden, Verfügbarkeitsprobleme, Mehraufwand zur Absicherung der Systeme
15	Ausfall der übergeordneten Stromversorgung (Energiemangellage)	flächendeckenden Stromausfall oder sonstige wesentliche techn. Gebrechen für > mind. 30min	Ausfälle von Services/ Dienstleistungen für ca. 360 %h

Tabelle 10: Mittel hohe Einzel- und (in hellrot) Dauerrisiken

8.2.1 RISIKO NR. 1, AUSFALL WESENTLICHER INFRASTRUKTUREN ODER BETRIEBSMITTEL

Aggregation: Dieses Risiko setzt sich aus den 11 Einzelrisiken zusammen.

Risikotyp: Eventrisiko

Zusammenfassung: Dieses Risiko adressiert menschliches Versagen sowie den möglichen Ausfall von wesentlichen Infrastrukturen durch Naturgefahren aller Art, durch technische Gefahren und Unzulänglichkeiten bei Gebäudeinfrastrukturen, die kritische Betriebsprozesse betreffen. Dieses Aggregationsrisiko integriert auch ein neu hinzugekommenes Risiko Nr. 142, *Versagen des präventiven Brandschutzes*.

Mögliche wesentliche Schadwirkungen: Dieses Risiko beschäftigt sich mit der Verfügbarkeit bzw. Ausfall von wesentlichen Dienstleistungen, bedingt durch Infrastrukturversagen im weitesten Sinn.

Unmittelbar zugeordnete Empfehlungen: Aus den Einzelrisiken zu Aggregationsrisiko 1 lassen sich folgende Empfehlungen ableiten:

- Eigentlich eine Selbstverständlichkeit: Redundanzen und physikalische Distanzen in der Leitungsführung für kritische Komponenten beachten. In diesem Kontext ist es wichtig darauf hinzuwirken, dass die Qualität der Offenlegung der tatsächlichen Infrastrukturen (insbesondere bei Hoch – und Tiefbau) ggfs. vertraglich abgesichert bzw. regelmäßig eingefordert/überprüft werden sollte; Einforderung von Infrastrukturstatus (regelmäßige Einforderung von Informationsupdates)
- Der Ausfall von wesentlichen Infrastrukturen muss im Störungs- Notfall- und Krisenmanagement Berücksichtigung finden
- Es wird empfohlen, alle relevanten vorhandenen Gefahrenkataloge bei der Beurteilung der Risiken von Standorten und Leitungen zu benutzen (z. B. Hochwasserrisikoanalyse, ZAMG-Klimakatalog, Eurocode-8 etc.). Eine Pflege eines solchen Katalogs wird bei ISPA angeregt.

8.2.2 RISIKO NR. 4, MÖGLICHE, ERHEBLICHE DEFIZITE BEI IKT-DESIGN UND SYSTEMARCHITEKTUR

Aggregation: Dieses Risiko setzt sich aus den 11 Einzelrisiken zusammen.

Risikotyp: Eventrisiko

Zusammenfassung: Dieses Risiko adressiert die Ungewissheit der technischen Innovationen bei ISPs und TELKOs mit Blick auf die prognostische Auslegung von IKT-Infrastrukturen. Hier werden die Entwicklungen sowohl bei Hard- und Software, beim Ausbau der Netze und die rasanten Umstrukturierungen bei IoT bzw. im Endkundenbereich und die damit verbundenen unbekannten neuen Herausforderungen subsummiert.

Mögliche wesentliche Schadwirkungen: Dieses Risiko beschäftigt sich mit möglichen unerwarteten negativen Entwicklungen z. B. techn. Overload durch Planungs- und Designfehler in der Gesamtheit. Einen wesentlichen Aspekt dabei spielen auch die ggfs.

unausgereiften und/oder zu rasch veraltenden Protokolle bzw. mögliche nicht bekannte negative Kaskadeneffekte bei der Einführung von neuen Protokollen (wie z. B. massiver Einsatz von Virtualisierungstechnologie wie Network Slicing, SDN, NFV etc.). Grundsätzlich wurde dieses Risiko im Zuge der 5G Risikoanalyse V3-2020 intensiv diskutiert. Das grundlegenden Herausforderungen bei Design- und Architektur haben sich jedoch nicht verändert. Daher blieben auch die grundlegenden Aussagen und Empfehlungen unverändert.

Unmittelbar zugeordnete Empfehlungen: Aus den Einzelrisiken zu Aggregationsrisiko 4 lassen sich folgende Empfehlungen ableiten:

> Obwohl hier mehrere Empfehlungen unmittelbar zugeordnet werden können, steht doch die Verfügbarkeit von Expert*innen für Planung und Designfragen im Fokus. Parallel dazu wird insbesondere die enge Abstimmung in der Branche, wie mit neuen Herausforderungen auf eine nicht wettbewerbsverzerrende Art und Weise reagiert werden soll und kann, angeregt. Die eingerichtete Expert*innengruppe, die sich mit den hier zusammengefassten Risiken beschäftigt hat, könnte unter Einbindung des Regulators einen wesentlichen Beitrag leisten (Aufbau eines PPP-Modells zur Abstimmung von techn.-organisatorischen Sicherheitsfragen)

8.2.3 RISIKO NR. 5, NEGATIVE AUSWIRKUNGEN VON POLITISCH/ RECHTLICHEN VORGABEN AUFGRUND SICH ÄNDERNDEN RAHMEN-BEDINGUNGEN AUCH ÖFFENTLICHE WAHRNEHMUNG

Aggregation: Dieses Risiko setzt sich aus 9 Einzelrisiken zusammen.

Risikotyp: Eventrisiko
Zusammenfassung: Dieses Risiko adressiert mehrere Aspekte:

- Mängel im zeitnahen Datenaustausch zur Abwehr von Angriffen sowie die Gefahr, dass techn. Innovationen, die der Sicherheit dienen, bei CPE nicht eingeführt werden
- Gefahr der mangelnden Koordination zwischen den Branchen zu IT-Security-Themen
- Gefahr der Angreifbarkeit durch die fehlende Zulässigkeit von Verkehrsprofilen
- Gefahr, dass Änderungen an der nationalen/internationalen Gesetzeslage notwendige Anpassungen von Security-Aspekte erheblich erschweren
- Gefahr, dass durch behördliche Auflagen absichtliche Schwachstellen in Sicherheitsmechanismen eingebaut und/oder ausgenutzt werden (müssen)
- Gefahr, dass regulatorische und rechtliche Einschränkungen den technischen Fortschritt limitieren
- Unerkannte Nebeneffekte bei behördlich angeordneten Internetsperren

Mögliche wesentliche Schadwirkungen: Im Wesentlichen beschäftigen sich die möglichen Schadwirkungen der o. a. angeführten Punkte mit einem unabsehbaren Mehraufwand für die Betreiber bei der Implementierung von Sicherheitsmechanismen, die in weiterer Folge erheblich negative Auswirkungen auf die Verfügbarkeit, Vertraulichkeit und Integrität von angebotenen Service- und Dienstleistungen haben können.

Unmittelbar zugeordnete Empfehlungen: Aus den Einzelrisiken zu Aggregationsrisiko 5 lassen sich folgende Empfehlungen ableiten:

- Anpassung von Rechtsvorschriften, um effiziente und koordinierte Abwehr von Cyberangriffen zu ermöglichen, wird auch durch NIS2 nicht abgedeckt
- Haftungsfragen rechtlich klären, regulatorische Vorgaben im Hinblick auf Netzneutralität ggfs. die Ergebnisse der EU-Regelungen einarbeiten nach Inkrafttreten der Maßnahmen des CRA wird dieses Risiko neu beurteilt
- Intensivierung des Datenaustausches über die kommenden Meldestellen, Aufbau von Branchen CSIRTs, Organisation von TLP-RED-Runden. Wird durch NIS2 voraussichtlich stark vermindert
- Frühzeitige Einbindung der Branche in die Gesetzgebung. Wird durch NIS2 voraussichtlich stark vermindert
- Alternative Gesetzesvorgaben für Überwachung anbieten
- Rechtssicherheit durch Anpassung der Gesetzeslage
- Aktive Bekämpfung von Fake News, ggfs. wissenschaftliche Auseinandersetzung
- Intensiver Austausch mit den TELKO/ISPs und politische Gremien Für alle anderen Punkte wird die frühzeitige Einbindung der Branchen in regulativen, rechtlichen und normativen Vorgaben angeregt. Dies bedeutet einerseits die Stärkung des hier begonnenen PPP-Prozesses, anderseits verpflichtet es die Unternehmen auch Ressourcen für die Erarbeitung der Rahmenbedingungen bereitzustellen.

8.2.4 RISIKO NR. 6, UNZUREICHENDE BERÜCKSICHTIGUNG VON ISMS-ANFORDERUNGEN IM BESCHAFFUNGSPROZESS

Aggregation: Dieses Risiko setzt sich aus 5 Einzelrisiken zusammen.

Risikotyp: Eventrisiko

Zusammenfassung: Dieses Risiko beschreibt die Herausforderungen bei der Durchsetzung von Securityanforderungen im Beschaffungsprozess, die primär möglichen mangelnden Spezifikationen und/oder organisatorischen Defiziten geschuldet sind.

Mögliche wesentliche Schadwirkungen: Fehlende Berücksichtigung von ISMS Anforderungen bei Beschaffungen können zu einem erheblichen Mehraufwand durch Workarounds im Betrieb führen; ggfs. überhaupt zur Nichtimplementierung von Teilaspekten zur IKT-Sicherheit.

Unmittelbar zugeordnete Empfehlungen: Aus den Einzelrisiken zu Aggregationsrisiko 6 lassen sich folgende Empfehlungen ableiten:

- Eine Gleichgewichtung von Security-Anforderungen mit funktionalen Anforderungen in der Ausschreibung/Beschaffung ist grundsätzlich anzustreben. Eine Einbindung von Security-Sachverstand in den Ausschreibungs-/Beschaffungsprozess ist obligatorisch
- Die Branche empfiehlt hier, dies insbesondere bei öffentlichen Ausschreibungen entsprechend zu berücksichtigen, da dies i.R. Vorbildwirkung hat.

- Entsprechende Mindestsicherheitsstandards auf EU-Ebene definieren
- Offenlegung von Non-Compliances, bei Komponenten. Umsetzung der EU-Richtlinien Cyber Resilience Act etc., 5G etc.-Zertschema
- Dieses Risiko muss ins Organisations-Lieferantenmanagement mit aufgenommen werden

8.2.5 RISIKO NR. 7, MANGELHAFTES NOTFALL-, KRISEN- UND KONTINUITÄTSMANAGEMENT

Aggregation: Dieses Risiko setzt sich aus den 8 Einzelrisiken zusammen.

Risikotyp: Eventrisiko

Zusammenfassung: Dieses Risiko schließt sich an das Risiko Nr. 12 an und adressiert alle Herausforderungen in der Eskalationsfähigkeit der Organisation bei Anomalien, Störungen und Notfällen bis hin zu Krisen.

Mögliche wesentliche Schadwirkungen: Mangelhaftes bzw. ungenügendes Training im Störungs-, Notfall- und Krisenmanagement verlängert die Bewältigung von Sicherheitsangelegenheiten/-vorfällen bei Vertraulichkeit, Verfügbarkeit und Integrität.

Unmittelbar zugeordnete Empfehlungen: Aus dem Aggregationsrisiko 7 lassen sich folgende Empfehlungen ableiten:

- Bewusstseinsbildung bei der obersten Leitung für die Notwendigkeit eines umfassend ausgestalteten Business Continuity Managements
- Awareness-Maßnahmen bei den Mitarbeitern, Lessons Identified und Lessons Learned Prozess aufsetzen (PDCA Kreislauf durchlaufen)
- an einschlägigen Übungen teilnehmen und qualifiziertes Personal einsetzen
- sinnvolles Clustern von Tickets
- Vorhalten, Prüfen und Einsatz von angepassten bzw. nötigen Ressourcen zur Ereignisbewältigung
- Kontinuierliche Auswertungen von Monitoring und Loggings durch Einsatz von SIEM-Tools
- Anpassung der Auswertungssichten auf die Logs / Setzen von Thresholds, um mögliche Störungen / Vorfälle rechtzeitig erkennen zu können
- Regelmäßige Restoretests aller relevanten Daten mit entsprechender Umsetzung der Policy
- Gemeinsam abgestimmte Öffentlichkeitsarbeit in der Branche/Medienarbeit
- Durchführen von Übungen, die über KPIs ausgewertet werden können, bis hin zu „Red and Blue Team Exercises“
- gerichtsfeste Dokumentation und Schulungen in dieser Hinsicht vorsehen

8.2.6 RISIKO NR. 8, ERHEBLICHE PROBLEME BEIM PATCH- UND UPDATE-PROZESS

Aggregation: Dieses Risiko setzt sich aus 9 Einzelrisiken zusammen.

Risikotyp: Eventrisiko

Zusammenfassung: Dieses Risiko erfasst die Herausforderungen und Problemstellungen bei Patch- und Updateprozessen aller Art. Dieses Risiko wurde de facto 1:1 aus der Betrachtung aus 2020 übernommen.

Mögliche wesentliche Schadwirkungen: Gefahr, dass sich beim Patchen/Updaten unerwartete Inkompatibilitäten zwischen Hard- und Software bzw. Software/Software ergeben, die primär in produktiven Umgebungen und nur unter bestimmten Lastbedingungen auftreten. Damit verbunden bereiten neu eingespielte Software/Updates erhebliche Schwierigkeiten, die auch mit dem Ausfall von Services verbunden sein können. Parallel dazu besteht die Möglichkeit der ungewollten öffentlichen Erreichbarkeit von Diensten aus dem Internet und damit verbundene Datenschutzverletzungen nach einem Updatezyklus. Eine weitere Schadwirkung beschäftigt sich damit, dass in Umkehrung zu obigen Aussagen auch nicht eingespielte Patches/Updates zu erheblichen Schadwirkungen bei Verfügbarkeit, Vertraulichkeit und Integrität führen können.

Unmittelbar zugeordnete Empfehlungen: Aus den Einzelrisiken zu Aggregationsrisiko 8 lassen sich folgende Empfehlungen ableiten:

- Forderung an die Hersteller und Lieferanten, eine klare Trennung von Security- und funktionalen Patches inkl. Haftungsübernahme durch die Lieferanten/Hersteller vorzusehen
- Relevanz- und Impactüberprüfungen und ggfs. Teststellungen im Einzelfall sowie Roll-out-Planung inkl. Fall-back-Szenarien erarbeiten und entsprechend intensiviert testen.
- Changemanagementprozesse einführen, fortschreiben und ggfs. den Erfahrungsaustausch zwischen den Organisationen intensivieren. Entsprechende Testsysteme, Tests und Rückstiegspläne, z. B. Open-Source-Lösungen prüfen, Kontinuitätsplanung inkl. Ressourcenplanung

8.2.7 RISIKO NR. 9, DEFIZITE BEI IDENTITY AND USER ACCESS CONTROL (IAM)

Aggregation: Dieses Risiko setzt sich aus den 12 Einzelrisiken zusammen.

Risikotyp: Eventrisiko

Zusammenfassung: Dieses Risiko fasst im Wesentlichen folgende Aspekte der Zugriffskontrolle zusammen:

- Mögliche mangelnde Securityregelungen bei Zugriff auf Betriebssysteme bzw. Systeme
- Unerkannte bzw. und /oder unerlaubte Ausübung von Rechten
- Lack of User Authentification Methods, insbesondere bei Legacy Equipment
- Zugriff von Testsystemen auf Produktivdaten und vice versa
- unerkannte Einfallstore auf die eigene IKT-Infrastruktur
- möglicher Missbrauch von Rechten

Auch in diesem Risiko wurden in den Einzelrisiken nur kleine Formulierungsänderungen durchgeführt.

Mögliche wesentliche Schadwirkungen: Mit den hier zusammengefassten Einzelrisiken sind immer erhebliche Einschränkungen bei Verfügbarkeit, Integrität, Vertraulichkeit mit zum Teil hohem Imageschaden für die betroffene Organisation verbunden. Darüber hinaus werden mögliche Datenschutzverletzungen und der damit verbundene Imageverlust sowie Strafen/Sanktionen angesprochen. Parallel dazu stellen überhaupt fehlende User-Access-Mechanismen, insbesondere bei Legacy Systemen einen hohen möglichen Multiplikationsfaktor dar, eigene(s) Netz(e) zu kompromittieren.

Unmittelbar zugeordnete Empfehlungen: Aus den Einzelrisiken zu Aggregationsrisiko 9 lassen sich folgende Empfehlungen ableiten:

- Sensibilisierung im Management, Segregation of Duties, Automatisierungen im User Management inkl. regelmäßige Reviews der Berechtigungen.
- Einführung und Implementierung eines entsprechenden ISMS z. B. ISO 27.001 mit den Controls der ISO 27.002 insbesondere Kap.9, Access-Control-Controls
- Need-to-know-Prinzip durchgängig in der Organisation umsetzen
- Entsprechendes Asset-Management und ggfs. ein Bewusstsein für die Substitution von Legacy Equipment schaffen
- Testen und Monitoring bewusst intensivieren
- Dort, wo möglich und sinnvoll, Zweifaktoren Authentisierung vorsehen
- Regelmäßige Audits zum Thema, falls nicht von ISMS abgedeckt

- Implementierung von Security-Policies (Festlegung von Erlaubten/Verbotenen), Einführen ISMS Angepasste SIEM-Systeme einsetzen. Entsprechendes Rechtemanagement einführen, regelmäßige Audits,
- Standards beim Verlassen von Mitarbeiter*innen einhalten

8.2.8 RISIKO NR. 11, AUSFALL/ERHEBLICHE SERVICEEINSCHRÄNKUNGEN BEI SINGULÄREN IKT-LIEFERANTEN ODER HERSTELLERN

Aggregation: Dieses Risiko setzt sich aus 3 Einzelrisiken zusammen.

Risikotyp: Eventrisiko

Zusammenfassung: Dieses Risiko fasst im Wesentlichen die unerwünschte Abhängigkeit von Herstellern und Lieferanten zusammen.

Mögliche wesentliche Schadwirkungen: Mit singulären Lieferanten und Herstellern gehen folgende mögliche Schadwirkungen einher:

- Möglicher hoher Multiplikationsfaktor bei Bekanntwerden und / oder Ausnutzung von funktionalen Einschränkungen; damit verbunden hohe betriebliche Einschränkungen, Verlust der Integrität, Verlust der Vertraulichkeit
- Nichteinhaltung von versprochenen funktionalen Fähigkeiten von Soft- und Hardware, die mangels Alternativen durch erhöhten Aufwand im Betrieb substituiert werden müssen
- Bei Ausfall von Dienstleistungen erhebliche Verzögerungen bei der Wiederherstellung eines definierten Regelbetriebs

Unmittelbar zugeordnete Empfehlungen: Aus den Einzelrisiken zu Aggregationsrisiko 11 lassen sich folgende Empfehlungen ableiten:

- Grundsätzliche Vermeidung von singulären Abhängigkeiten, z.B. eine zwei Vendor Strategie evaluieren
- Einkaufspolitik; Upgrade-Zyklus anpassen; weg von Single-Vendor-Policy hin zu Multi – Vendor; Vorhaltung von (kritischen) Ersatzgeräten und deren Überprüfung. Eine ABC-Logistik einführen.
- Pönalen, Lieferantenauswahl (Bonitätsprüfung etc.); Vorhalten von Ersatzteilen; Zwei Vendorstrategien prüfen;
- Alternative Kommunikationswege mit wichtigsten Herstellern aufbauen. Laufende Strategie- und Bonitätsprüfung von Herstellern und Lieferanten, die in die Kategorie „singulär“ einzuordnen wären.
- Laufende Marktbeobachtung, damit verbunden Bereitstellung von Ressourcen, um die Marktbeobachtung auch durchzuführen.
- Vorhalten von Ersatzteilen und/oder Support daher: Logistikkonzept anpassen und nach Möglichkeit die Abhängigkeit von einem singulären Lieferanten vermeiden.
- Mit Blick auf die Nichteinhaltung von versprochenen Service/Funktionalitäten alternative Kommunikationswege mit den wichtigsten Herstellern aufbauen

8.2.9 RISIKO NR. 12, MÄNGEL IN DER BETRIEBSFÜHRUNG

Aggregation: Dieses Risiko setzt sich aus den 26 Einzelrisiken zusammen.

Risikotyp: Dauerrisiko

Zusammenfassung: Dieses Risiko adressiert alle Herausforderungen in der Betriebsführung und stellt daher ein Dauerrisiko dar. Selbstverständlich werden diese Risiken bei allen Betreibern entsprechend „gemanaged". Das Risiko wurde aufgrund der Zusammenschau aller Einzelrisiken mitaufgenommen, da es die branchentypischen Herausforderungen beschreibt. Dies gilt insbesondere für den gesamten Disaster Life-Cycle;

- Preparedness Measures mit Blick auf die Vorbereitung auf Störungen und Incidents
- Reaktionsmaßnahmen in situ mit der Verpflichtung, als Organisation eskalieren zu können
- und der Herausforderung, einen entsprechenden Lessons-learned bzw. Lessons-identified-Prozess mit in die tägliche Betriebsführung zu implementieren.

Mögliche wesentliche Schadwirkungen: In Summe werden hier erhebliche Betriebsstörungen und erheblicher monetärer Mehraufwand von Schäden durch zum Teil zu späte oder komplette Nichterkennung bzw. erhebliche Verzögerungen bei Erkennung von Angriffen und damit verbundener Verlust von Integrität/ Vertraulichkeit/Verfügbarkeit adressiert. Zusätzlich können erhebliche Probleme beim Incident-Response Reaktionszeiten verlängern, die in Summe wieder Schäden für die Organisation darstellen können.

Unmittelbar zugeordnete Empfehlungen: Aus dem Aggregationsrisiko 12 lassen sich folgende Empfehlungen ableiten:

- Entsprechendes Management der Informationssicherheit einführen
- Den Know-how-Level der (betriebsführenden) Mitarbeiter möglichst hochhalten.
- Kontinuierliche Auswertungen von Monitoring und Loggings durch Einsatz von SIEM-Tools
- Nutzung von entsprechenden Dokumentenmanagementsystemen bzw. Ressourcen für Dokumentation bereithalten, Auditierungen der internen Prozesse, Standards für die Dokumentation festlegen, einhalten und überprüfen
- Einbindung des Datenschutzbeauftragten und ISMS-Beauftragten in die Belange der Betriebsführung und Fortschreibung der Sensibilisierung des Managements für Security-Themen
- Bewusstseinsbildung bei der obersten Leitung für den Return on Invest von Securitymaßnahmen, Awarenessmaßnahmen bei den Mitarbeitern ständig updaten, Lessons-identified- und Lessons-learned-Prozess aufsetzen (PDCA Kreislauf durchlaufen)
- Schulungen der Mitarbeiter inkl. sauberes Priorisieren, Klassifizieren und Korrelieren von Alarmmeldungen
- Unangekündigte Simulationen durchführen, regelmäßige Überarbeitung der Alarmgaben

8.2.10 RISIKO NR. 15, AUSFALL DER ÜBERGEORDNETEN STROMVERSORGUNG (ENERGIEMANGELLAGE)

Aggregation: Dieses Risiko setzt sich aus 3 Einzelrisiken zusammen.

Risikotyp: Eventrisiko

Zusammenfassung: Dieses Risiko adressiert Stromausfallsszenarien aller Dimensionen. Das Risiko wurde zum Risiko Nr.1 klarer abgegrenzt und daher unbenannt.

Mögliche wesentliche Schadwirkungen: Dieses Risiko beschäftigt sich mit der Verfügbarkeit bzw. Ausfall von wesentlichen Dienstleistungen, bedingt durch den Wegfall des Kernbetriebsmittels Strom.

Unmittelbar zugeordnete Empfehlungen: Aus den Einzelrisiken zu Aggregationsrisiko 15 lassen sich folgende Empfehlungen ableiten:

- Die USV-Zeiten nach einem entsprechenden TIER-Modell auslegen und adäquate elektrotechnische Vorkehrungen treffen
- Bei der Notstromversorgung darauf achten, dass auch die Anschlussversorgung mit Diesel gesichert ist.
- Entsprechende Umschalttest sowie BCM-Pläne für Fehler vorhalten und beüben

8.3 Übersicht der geringen Aggregationsrisiken

Es wurde nur ein Aggregationrisiko in diese Gruppe aufgenommen

8.3.1 NR. 14, MANGELNDE COMPLIANCE (DATENSCHUTZ, STANDARDS, VERTRÄGE ETC.) ODER FEHLENDE LEGISTIK

Aggregation: Dieses Risiko setzt sich aus 10 Einzelrisiken zusammen.

Risikotyp: Eventrisiko

Zusammenfassung: Dieses Risiko beschreibt im Wesentlichen die Gefahr der ungewollten Nichteinhaltung von Rechtsvorgaben aufgrund von denkbaren organisatorischen Defiziten und die Rechtsunsicherheit durch einen Interpretationsspielraum bei Formulierungen in Durchführungsverordnungen. Selbstverständlich werden mögliche Verletzungen von SLAs und damit verbunden Pönale sowie mögliche Datenschutzverletzungen ebenfalls unter diesem Risiko subsumiert.

Mögliche wesentliche Schadwirkungen: Abgesehen von ungewollter Veröffentlichung von schützenswerten Informationen stehen die drohenden Strafen durch die Datenschutzgesetze im Vordergrund der Risikobeschreibung.

Unmittelbar zugeordnete Empfehlungen: Aus den Einzelrisiken zu Aggregationsrisiko 14 lassen sich folgende Empfehlungen ableiten:

- Nachweis der Wirksamkeit eines umfassend ausgestalteten Risikomanagements
- Einführung eines Dokumentenmanagementsystems und Bereitstellung entsprechender Ressourcen für die Dokumentation
- Regelmäßige Auditierungen der Einhaltung von Standards für die Dokumentation
- Normative Dekommissionierungsprozesse einführen

9. Veränderungen in der Risikolandschaft

Am übersichtlichsten werden die Veränderungen des Risikoportfolios in der Telekommunikationsbranche anhand der Änderungen bei den Aggregationsrisiken aufgezeigt.

In der Version V 2.0 -2019 wurden 14 Aggregationsrisiken formuliert. In der Betrachtung aus 2020 wurde ein neues Aggregationsrisiko hinzugefügt. Dieses hinzugefügte Aggregationsrisiko Nr. 15 beschäftigte sich in der Version 3.0-2020 mit dem Ausfall wesentlicher Betriebsmittel. Dieses wurde beibehalten und in der Risikohöhe nicht verändert. Es enthält aber im Vergleich zu V3.0 nur mehr Stromversorgungsthemen. Insofern wurde das Risiko stärker abgegrenzt.

Eine wesentliche Veränderung gab es im Vergleich zu 2020. Das Risiko Nr.3, kriminelle Handlungen aus dem Cyberraum sowie Cyber-Fraud, hat in den letzten Jahren deutlich an

negativer Bedeutung zugelegt. Es wird daher aus derzeitiger Sicht als ein Dauerrisiko mit erheblich negativen Auswirkungen eingeschätzt, die für unzählige betroffenen Unternehmen auch dramatisch hohe monetäre Aufwendungen nach sich ziehen.

Im Dauerrisiko Nr. 2 wurden die monetären Schäden mit in die Aggregation aufgenommen.

Da Risiko Nr. 10, Verlust der Vertraulichkeit von geschützter Information, wurde im Vergleich zu 2020 auch monetär bewertet. Durch die sicherheitspolitischen Veränderungen in den letzten drei Jahren hat sich die Intensität der Wirtschafts- und Industriespionage erhöht. Es wird durch die Aufnahme in den Risikokatalog ein hinweisendes Zeichen gesetzt. Die genauen Schadenshöhen lassen sich schwer auf eine einzelne Organisation herunterbrechen.

9.1 Vergleich der Aggregationsrisiken V3-2020 zur aktuellen Einschätzung

In der V3-2020 war ein Schwerpunkt auf der Einführung der 5G-Technologie gelegt worden.

Obwohl die meisten Aggregationsrisiken hier unverändert erscheinen, wurden bei den Einzelrisiken 21 Risiken gelöscht und 3 Einzelrisiken hinzugefügt.

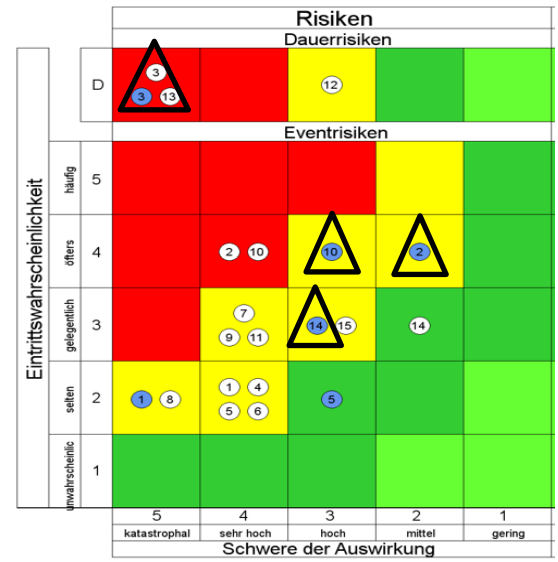

Abbildung 10: Aggregationsrisiken V4.0-2023

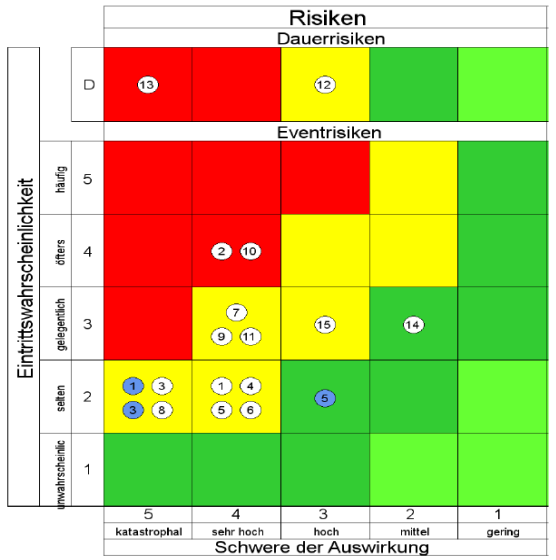

Abbildung 11: Aggregationsrisiken V3.0-2020

In der nachfolgenden Abbildung wird der Verlauf der Entwicklung seit 2019 visualisiert.

9.2 Verlauf der Risikoeinschätzungen seit 2019 (immer Worst Case)

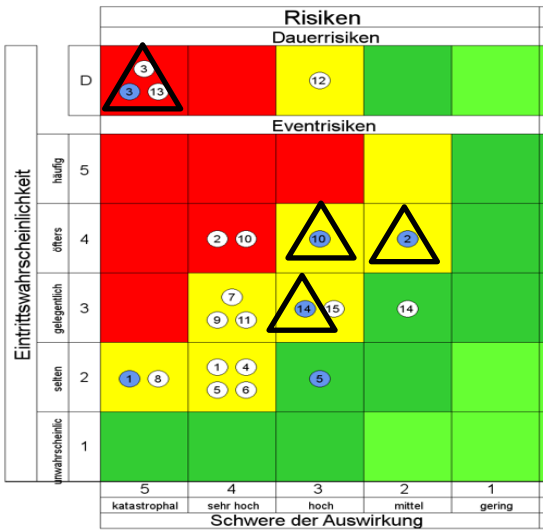

Abbildung 12: Aggregationsrisiken V4.0-2023

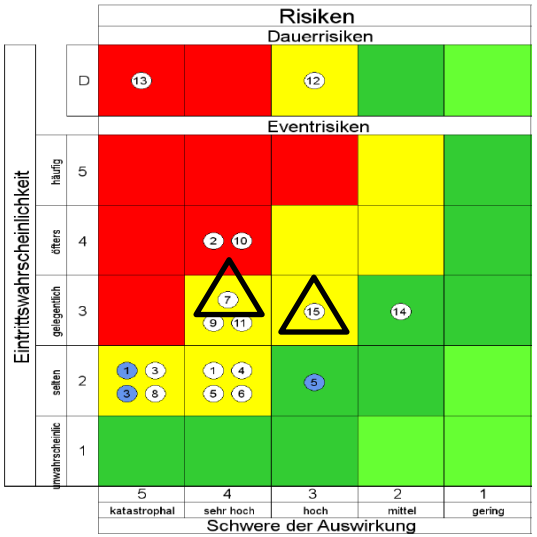

Abbildung 13: Aggregationsrisiken V3.0-2020

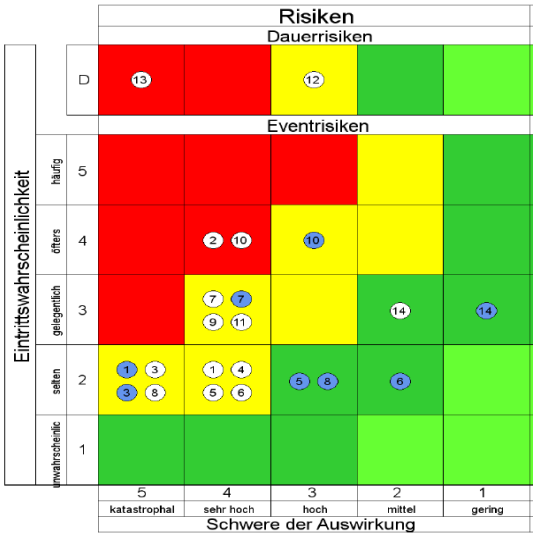

Abbildung 14: Aggregationsrisiken V2.0-2019

9.3 Auswertung und Vergleich der Risikokategorien

Basis der Verteilung der Risikokategorien sind 113 Einzelrisiken im Vergleich zu 131 aus 2020. Grüne Dreiecke signalisieren einen Rückgang der Einzelrisiken in der jeweiligen Risikokategorie. Dies ist im Wesentlichen der Gesamtreduktion der Einzelrisiken geschuldet. Rote Dreiecke signalisieren einen Anstieg im Vergleich zu 2020. Analysiert man die Risikokategorien gibt es eine **klare Zunahme** bei den kriminellen Gefahren, da die zugrunde liegende Gesamtzahl an Einzelrisiken um ca. 14% reduziert wurde. In der Risikokategorie Technik wurde umstrukturiert und es wurden Risiken hinzugefügt. Damit erklärt sich der Anstieg in dieser Kategorie.

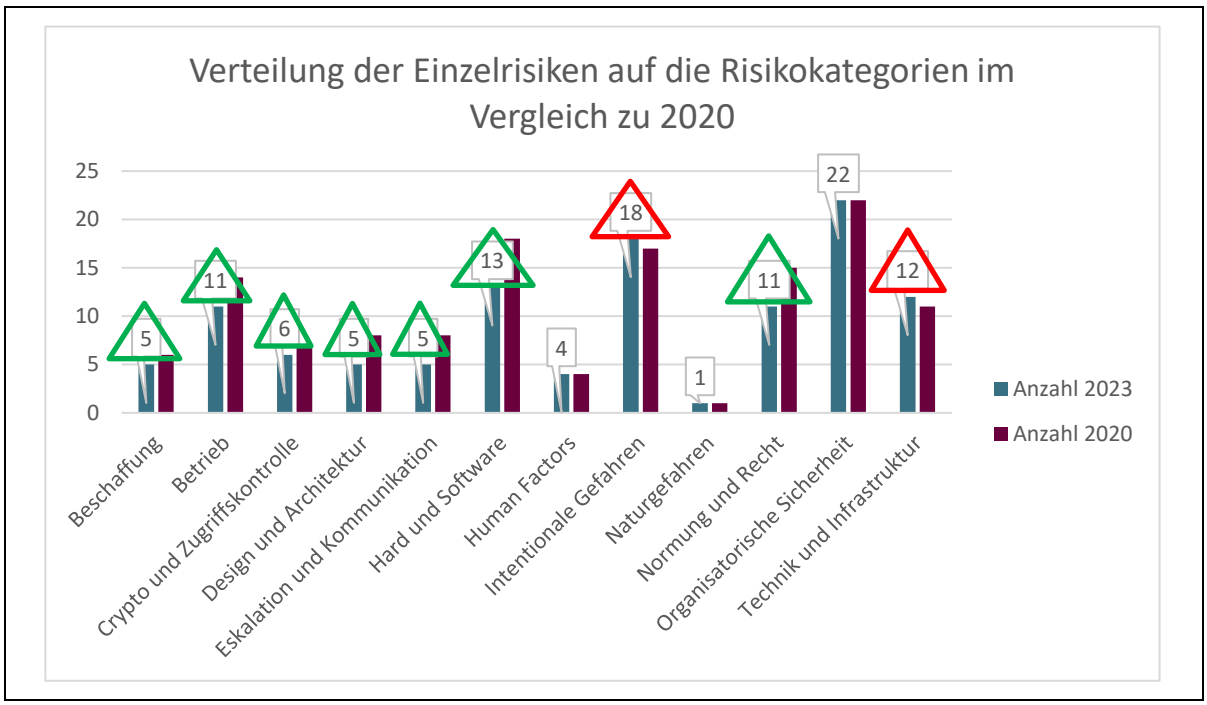

Abbildung 15: Darstellung der Verteilung der Risikokategorien im Vergleich zu 2020

Teil IV Maßnahmen & Empfehlungen

10. Empfehlungen

Die nachfolgenden Empfehlungen leiten sich aus mehreren Perspektiven ab und fassen die Ergebnisse der Expert*innenworkshops im Jahr 2023 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. 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 innerhalb der Organisation, zwischen den Organisationen 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

Im Rahmen der Empfehlungen werden 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 den Umsetzungsstand dem Lenkungsausschuss der RTR-IKT-Branchenrisikoanalyse im Rahmen einer periodischen Revision 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 Jahre benötigen

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

10.3 Übersicht der Änderungen in den Empfehlungen

Aus den 12 Risikokategorien wurden 28 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 » BCM (wird nur in den Empfehlungen genutzt) » Naturgefahren » Normung und Recht

Diese verteilen sich auf folgende Risikokategorien wie nachstehend abgebildet:

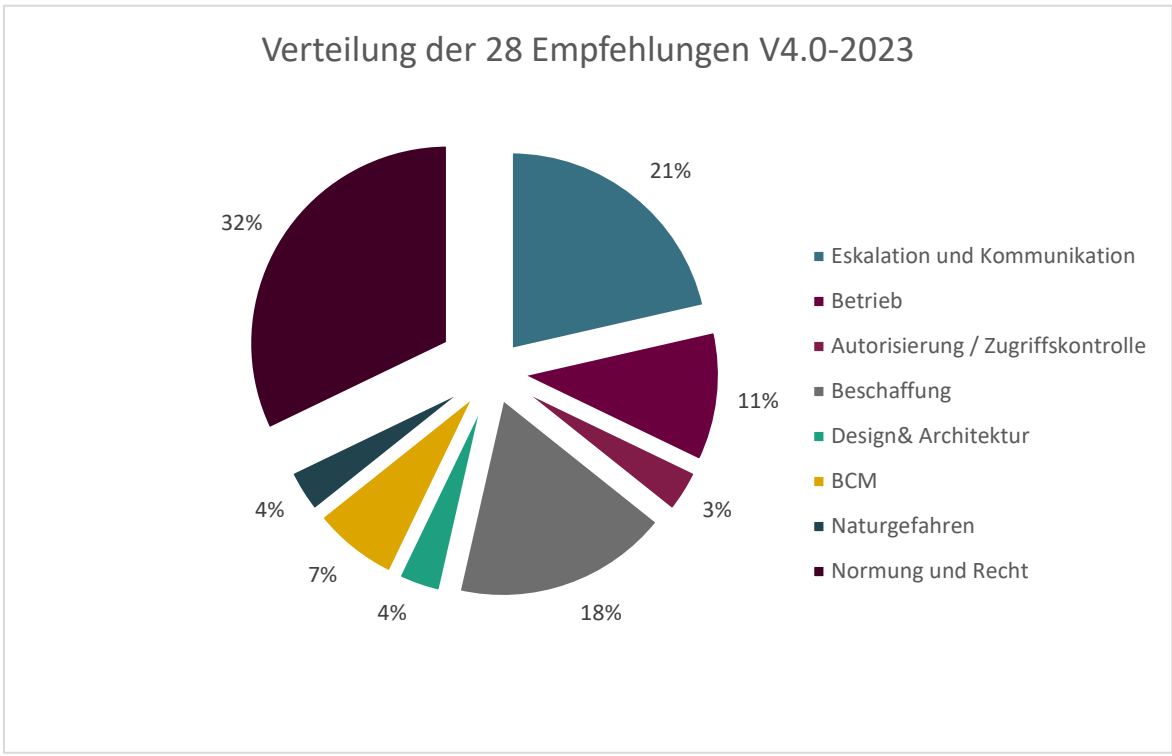

Abbildung 16: Verteilung der Empfehlungen auf die Risikokategorien V4-2023

Ein Drittel der Empfehlungen finden sich in der Risikokategorie Betrieb

In Version V3.0-2020 der Risikoanalyse wurden 31 Empfehlungen formuliert. Es wurden folgende Empfehlungen gelöscht, da sie inzwischen durch gesetzliche Vorgaben abgedeckt werden. Es sind dies folgende Empfehlungen:

Nr.	Empfehlung geordnet nach aufsteigender Nummer	Prozess-eigner	Priorität
~~9~~	~~Es wird empfohlen ein ISMS zu betreiben~~	~~TELKO/ ISP~~	~~1~~
~~11~~	~~Es wird empfohlen Awarenesskampagnen betreffend Social-Engineering / Phishing - insbesondere im Management der Organisationen regelmäßig durchzuführen.~~	~~TELKO/ISP~~	~~1~~
~~18~~	~~Ein CIRS-Modell (Critical Incident Reportingsystem) bei innerbetrieblichen "Fehlentscheidungen" für "Beinahe"-Vorfälle wird empfohlen. (Keine Weitergabe von Information an Externe Dritte)~~	~~TELKO/ISP~~	~~3~~
~~28~~	~~Es wird empfohlen Dekommissionierungsprozesse für die sichere Löschung von schützenswerten Daten bzw. die Zerstörung von Datenträgern/Datenspeicher zu schaffen.~~	~~TELKO/ISP~~	~~1~~

Tabelle 11: Gelöschte Maßnahmen

10.3.1 GEGENÜBERSTELLUNG DER EMPFEHLUNGEN V3.0-2020 ZU V4.0-2023

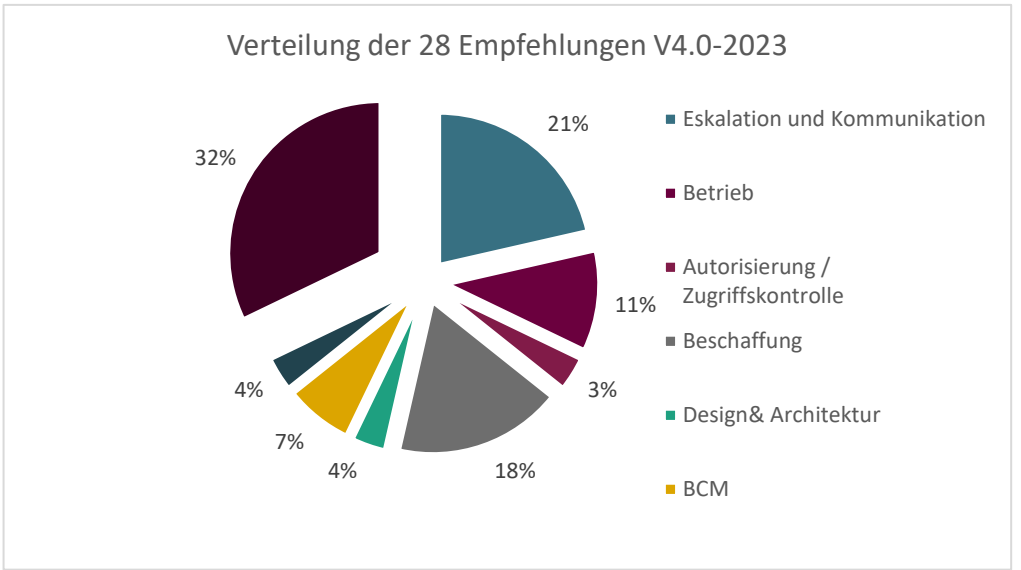

Abbildung 17: Verteilung der Empfehlungen auf die Risikokategorien V4-2023

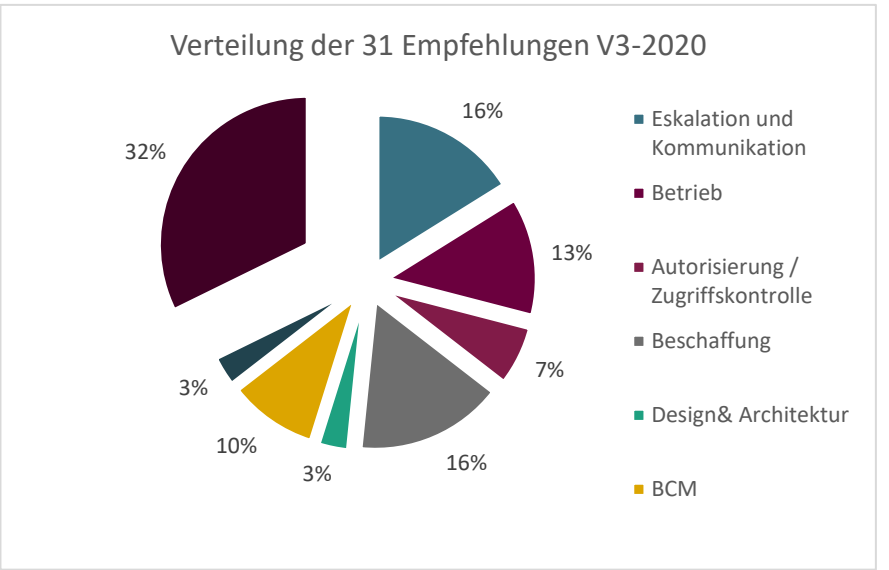

Abbildung 18: Verteilung der Empfehlungen auf die Risikokategorien V3-2020

11. Beschreibung der Empfehlungen

11.1 Eskalation und Kommunikation

Kategorie	Nr.	Empfehlung geordnet nach aufsteigender Nummer	Prozess-eigner	Priorität	Anmerkung	Zuordnung zu Aggregations-risiko	Aufwands-schätzung /a
Eskalation und Kommunikation	1	Die „Einrichtungen“ sollten eine (24/7/365) erreichbare Krisenmeldestelle haben. Diese dient als SPOC (Single Point of Contact) für Behörden, und für andere KIs	TELKO /ISP	1	Innerbetriebliche Entgegennahme von Meldungen mit der Möglichkeit innerbetrieblich eskalieren zu können	1,2,3,7,12,13,15	n.a.
	2	Um für Störungen, Notfälle und Krisen eine einheitliche Denk- und Handlungsweise in Österreich umzusetzen, müssen die Verfahren des SKKMs in den Organisationen bekannt sein. Es wird daher angeregt, dass die Unternehmen einen repräsentativen Personenkreis einer SKKM oder vergleichbaren Ausbildung zuführen.	TELKO /ISP/ BM.I	1	z.B. operativ tätige Personen oder Mitglieder im Krisenstab sollten die Verfahren kennen sollten an SKKM-Ausbildungen teilnehmen	7	10-20PT
	3	In Anlehnung an den BSI 200-4 und mit Blick auf die ISO 22.301 wird empfohlen mind. einmal im Jahr eine organisationsinterne Notfall-/Krisenübungen durchzuführen. Für relevante Betreiber wird dies mind. biannual empfohlen. Die Übungstype legt die Organisation intern fest und dokumentiert den Erfolg der Übung.	TELKO /ISP	1	Die Behörde kann ein angemessenes Übungsszenario festlegen. Bei der Übung wird die Wirksamkeit des BCM-Systems einmal jährlich erprobt.	7,1,2,3,15	15PT
	4	Es wird empfohlen, dass die NIS Behörde regelmäßig interorganisationale (Kommunikations-) Übungen durchführt und die entsprechenden Organisationen dazu einlädt.	BKA	1	Allen eingeladenen Organisationen wird empfohlen, solchen Einladungen zu folgen.	7	15PT
	5	Es ist die Prüfung zu initiieren, ob und wie eine autarke digitale Kommunikation zwischen Behörden und „Einrichtungen“ inklusive Benutzungsregeln, eine staatliche Notwendigkeit ist.	RTR	2	Analog dem ehemaligen Staatsgrundnetz	7	5PT

Kategorie	Nr.	Empfehlung geordnet nach aufsteigender Nummer	Prozess-eigner	Priorität	Anmerkung	Zuordnung zu Aggregations-risiko	Aufwands-schätzung /a
	6	Der Sektor übergreifende Informationsaustausch zwischen Betreibern und Behörden zur Bekämpfung bzw. Eindämmung von Cybercrime und dem dadurch verursachten Schaden soll rechtlich ermöglicht und technisch beschleunigt werden	BKA	1			

Tabelle 12. Empfehlungen zu Eskalation und Kommunikation

11.2 Betrieb

Kategorie	Nr.	Empfehlung geordnet nach aufsteigender Nummer	Prozess-eigner	Priorität	Anmerkung	Zuordnung zu Aggregations-risiko	Aufwands-schätzung /a
Betrieb	7	Es wird empfohlen alle Controls der ISO 27.002 sowie alle CIS-TOP20 oder vergleichbares wirksam in der Organisation zu berücksichtigen.	TELKO /ISP	2	Mit einer ggfs periodischen Überarbeitung des Betriebshandbuches	1,2,3,4,6,7,8,9,10 ,11,12,13	20PT
	8	Diskussion einer möglichen Verpflichtungs-aufforderung an Hersteller und Lieferanten für die Trennung und Kennzeichnung von funktionalen und Security relevanten Patches inkl. der nationalen Abstimmung für ein solches Vorgehen.	ENISA/ ISPA/ RTR/C SP	1	Das Ergebnis der Diskussion soll sich an die EU-Gesetzgebung richten	8	n.a.
	9	Es wird empfohlen, dass im Rahmen der KIRAS Sicherheitsforschung die Sinnhaftigkeit und Umsetzbarkeit einer nationalen und/oder internationalen Prüf- und Meldestelle für Hard- und Softwaresecurity untersucht wird.	ENISA/ RTR	3	Die Beteiligung von „Wesentlichen Einrichtungen“ an dieser Forschung wird erwartet. Ein Zertifizierungsschema durch ENISA wird erwartet.	13	n.a.

Tabelle 13. Empfehlungen zu Betrieb

11.3 Autorisierung/ Zugriffskontrolle

Kategorie	Nr.	Empfehlung geordnet nach aufsteigender Nummer	Prozess-eigner	Priorität	Anmerkung	Zuordnung zu Aggregations-risiko	Aufwands-schätzung /a
Autorisierung / Zugriffskontrolle	10	Die Umsetzung der Empfehlungen von "Applied Crypto Hardening, nach dem Stand der Technik wie z.B. https://bettercrypto.org", OWASP, etc wird empfohlen.	TELKO /ISP	1	Aufwand bezieht sich primär auf die Grundlagenerhebung nicht auf die Anwendung	4, 9, 10	10+ PT/a

Tabelle 14. Empfehlungen zu Zugriffskontrolle

11.4 Beschaffung

Kategorie	Nr.	Empfehlung geordnet nach aufsteigender Nummer	Prozess-eigner	Priorität	Anmerkung	Zuordnung zu Aggregations-risiko	Aufwands-schätzung /a
Beschaffung	11	Es ist eine Prüfung zu initiieren, ob die Bedingungen des ENISA Papers Indispensable Baseline Security Requirements for the Procurement of Secure ICT Products and Services in Österreich in dieser Form zur Anwendung gebracht werden können.	TELKO /ISP	1	Sollte von allen Einrichtungen beachtet werden.	6,11	5PT/a und zusätzlich 2+PT pro Beschaffung
	12	Es wird empfohlen die Entwicklung von Standards für eine sichere Konfiguration von CPEs und IoT-Devices in Österreich besser zu katalysieren. Hierzu sollten alle relevanten Dokumentationen wie z.B. Lit.RTR-19, https://www.telekom.com/resource/blob/314436/55257546f192be29b8159df115194bb0/dl-technische-sicherheitsanforderungen-data.zip herangezogen werden	RTR/CERT.AT /ISPA	1	Security by default, s. Paper DTAG, inklusive 5G Standards	4, 5, 13	25 PT

Kategorie	Nr.	Empfehlung geordnet nach aufsteigender Nummer	Prozess-eigner	Priorität	Anmerkung	Zuordnung zu Aggregations-risiko	Aufwands-schätzung /a
	13	Es wird empfohlen, dass Betreiber unterstützt werden Hersteller und Lieferanten zur geregelten Behandlung von Anfragen zu Sicherheitsschwachstellen zu verpflichten. Dies sollte möglichst harmonisiert erfolgen. (z.B. durch Musterrahmenvereinbarung)	ENISA/ ISPA/ RTR/C SP	1	Um kartellrechtliche Bedenken auszuräumen, wird hier eine Standardformulierung durch die Branche empfohlen vgl. dazu auch Punkt 3.8 des ENISA Papers Indispensable Baseline Security Requirements	13, 6	n.a.
	14	Die Sicherheitsanforderungen der Organisationen sind in allen Beschaffungsprozessen im jeweilig zutreffenden Ausmaß zu berücksichtigen	TELKO /ISP	2	gemeint sind Zugriff, Zutritt, auch elektronische Dienstleistungen etc	6	n.a.
	15	Lieferanten bzw. Hersteller von Soft- bzw. Hardware sollen dazu angehalten werden, rechtzeitig und angemessen auf bekanntgewordene Sicherheitsschwachstellen ihrer Produkte zu reagieren. Eine entsprechende Information soll an deren Kunden und an das nationale CSIRT zeitnah weitergegeben werden.	TELKO /ISPs/ BKA/R TR	1	Es wird angeregt bei öffentlichen Beschaffungsprozesse diese Forderung zu katalysieren	6,13	n.a.

Tabelle 15. Empfehlungen zu Beschaffung

11.5 Design und Architektur

Kategorie	Nr.	Empfehlung geordnet nach aufsteigender Nummer	Prozess-eigner	Priorität	Anmerkung	Zuordnung zu Aggregations-risiko	Aufwands-schätzung /a
Design& Architektur	16	Es wird eine institutionalisierte und Sektor übergreifende Zusammenarbeit im Risikomanagement, bei Informationssicherheits-management Themen sowie bei ISM-Designfragen angeregt, um so die Grundlagen für einen gemeinsamen Sicherheitsstandard zu schaffen.	TELKO /ISP	2		4	15 PT

Tabelle 16. Empfehlungen zu Design & Architektur

11.6 BCM

Kategorie	Nr.	Empfehlung geordnet nach aufsteigender Nummer	Prozess-eigner	Priorität	Anmerkung	Zuordnung zu Aggregations-risiko	Aufwands-schätzung /a
BCM	17	Es wird empfohlen, dass auch kleinere nicht dem NIS2.0 Regime unterworfenen Organisationen einen Informationssicherheitsbeauftragten (CISO) haben.	TELKO /ISP	1		12	n.a.
	18	Die arbeitsrechtliche Stellung des CISO im Unternehmen sollte es ermöglichen, effektiv dem ISMS nachzukommen und soll direkt der obersten Leitung der Organisation berichten.	TELKO /ISP	1	Koordinierung mit NIS Gesetz anstreben.	12	n.a.

Tabelle 17. Empfehlungen zu BCM

11.7 Naturgefahren

Kategorie	Nr.	Empfehlung geordnet nach aufsteigender Nummer	Prozess-eigner	Priorität	Anmerkung	Zuordnung zu Aggregations-risiko	Aufwands-schätzung /a
Naturgefahren	19	Es wird empfohlen, alle relevanten vorhandenen Gefahrenkataloge bei der Beurteilung der Risiken von Standorten und Leitungen zu benutzen (z. B. Hochwasserrisikoanalyse-HORA, ZAMG-Klimakatalog, Eurocode-8 etc.). Eine Pflege eines solchen Katalogs wird bei ISPA angeregt.	TELKO /ISP	1	Zusammenstellung von Gefahrenkatalogen im Bericht aufnehmen und anregen, dass ISPA diesen weiter pflegt und verdichtet. Referenzlisten erarbeiten.	1	5 PT

Tabelle 18. Empfehlungen zu Naturgefahren

11.8 Normung und Recht

Kategorie	Nr.	Empfehlung geordnet nach aufsteigender Nummer	Prozess-eigner	Priorität	Anmerkung	Zuordnung zu Aggregations-risiko	Aufwands-schätzung /a
Normung und Recht	20	Mit Blick auf die in §44 TKG geforderten Maßnahmen zur Erhaltung der Netzintegrität wird empfohlen, die Möglichkeit von Gerätesperren oder einen Quarantänestatus von Kundenendgeräten (insbesondere bei IoT, die z.B. durch mangelnde Updatemöglichkeiten betriebliche Probleme verursachen) durch den Betreiber vorzusehen, um Multiplikationsfaktoren im Netz durch Schwachstellen bei diesen Gerätetypen zu vermeiden. Es wird empfohlen diese Aspekte in den AGBs entsprechend zu berücksichtigen bzw. eine Mustervorgehensweise zu erarbeiten und Best-Practice-Modelle zu identifizieren.	TELKO /ISP/ISPA	1		3,12,14	20PT
	21	Es sollte geprüft werden, inwieweit der Betreiber entsprechende Monitoringmöglichkeiten zur Erkennung von Netzintegritätsverletzungen und Multiplikationsfaktoren durch Schwachstellen bei Kundenendgeräten hat.	RTR/ISPA/CERT.AT	1	Informeller Austausch zwischen RTR, CERT.AT und ISPA initiieren und Klarstellungen erwirken/erarbeiten. Problem Statement seitens CERT.AT.	12	n.a.
	22	Aus Sicht der Branche sind absichtliche Backdoors und Schwächungen von Sicherheitsmechanismen ein schweres Sicherheitsrisiko und werden daher klar abgelehnt.	TELKO /ISP	1	Diese Empfehlung zielt auf behördliche Begehren ab; Arbeitsbegriff "Staatstrojaner"	4,5,10,14	n.a.
	23	Es wird empfohlen, dass die Einbeziehung der Branche bei regulatorischen Vorgaben betreffend Überwachungsmaßnahmen und Beauskunftung in Bezug auf das Internet intensiviert wird.	BKA/BMI/BMF/BMJ /ISPA	1	Das Expert*innengremium der Risikoanalyse sowie Arbeitskreise der ISPA können genutzt werden	5,14	n.a.

Kategorie	Nr.	Empfehlung geordnet nach aufsteigender Nummer	Prozess-eigner	Priorität	Anmerkung	Zuordnung zu Aggregations-risiko	Aufwands-schätzung /a
	24	Es wird empfohlen, dass Österreich eine Mitwirkung und Unterstützung bei der Erarbeitung von Testregimen und Test- und Prüfmechanismen (ENISA-Prüfstelle) für undokumentierte, nicht erwartbare und schwer prüfbare Funktionen mit Datenabfluss bei Corekomponenten vorantreibt. RTR fungiert dabei als SPOC zur ENISA insbesondere im Kontext mit der Forderung nach einer "IKT-CE-Kennzeichnung"	ENISA/ RTR	1	ENISA Forschung soll unterstützt werden ggfs. auch durch die FFG,	13	n.a.
	25	Erarbeitung von Rahmenrichtlinien/Vorgaben dass Inverkehrbringer von IoT-Devices nur sicher konfigurierte Endgeräte ausliefern dürfen.	ISPA/E NISA	1	vgl. dazu Empfehlung 13 EU-Markt	3,12, 13	n.a.
	26	Es wird angeregt, die Strafanzeigen bei Cyberstraftaten für Wesentliche und Wichtige Einrichtungen zu vereinfachen.	BMI/CE RT.AT	1	Eine Strafanzeige bei Straftaten aus / im Cyberraum bei der nächsten Polizeidienststelle wird als nicht zielführend erachtet!	3	n.a.
	27	Es sollten Empfehlungen für Defaultklassen für Sicherheitsprofile/Einstellungen auf IPv6 (direkte Erreichbarkeit jedes Endgeräts) Kundenendgeräte eingeführt werden, um der Angreifbarkeit entgegenzuwirken. Zusätzlich sollten Firewalls standardmäßig aktiviert sein.	RTR/T ELKO/I SP	1		4,12	n.a.
	28	Eine Kostenanerkennung bei/von Betreibern von hoheitlich veranlassten sicherheitsrelevanten Ausgaben muss geprüft werden.	ISPA	1		5	n.a.

Tabelle 19. Empfehlungen zu Normung und Recht

Übersicht der Anhänge

Anhang 1: Allgemeines zu den Gefahrenkatalogen

Kurzbeschreibung der allgemeinen Gefahrenfelder

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.

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.

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.

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.

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.

GEFAHRENFELD-VI: COMMUNICATIONS SECURITY

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

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.

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.

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.

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.

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.

Anhang 2 Allgemeiner Gefahrenkatalog

Gefahrenfeld-I: baulich/physische Gefahren & umweltbezogene Gefahren

Gefahrenfeld-I baulich/physische Gefahren & umweltbezogene Gefahren				
Subkategorie	Nr.	Gefahren	Referenz	Bemerkung
Gefahren, die durch Defizite im Objektschutz entstehen können	GF-I-01	Gefahr der Brandstiftung	ENISA-GL-4.1.7	
	GF-I-02	Gefahr eines Hardware-Diebstahls	ENISA-GL-4.1.13	
	GF-I-03	Gefahr eines Kabeldiebstahls	ENISA-GL-4.1.14	
	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-07	Equipment	ISO-27002-11.2	
	GF-I-08	Großereignisse im Umfeld/Gefährdete Objekte/Nachbarn	BSI-IT-GS-G 0.5	
	GF-I-09	Ausspähen von Informationen / Spionage	BSI-IT-GS-G 0.5	
	GF-I-10	Abhören	BSI-IT-GS-G 0.5	
	GF-I-11	Diebstahl von Geräten, Datenträgern oder Dokumenten	BSI-IT-GS-G 0.5	
	GF-I-12	Verlust von Geräten, Datenträgern oder Dokumenten	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-14	Unbefugtes Eindringen in ein Gebäude	BSI-IT-GS-G 0.5	
	GF-I-15	Diebstahl	BSI-IT-GS-G 0.5	
	GF-I-16	Vandalismus	BSI-IT-GS-G 0.5	
	GF-I-17	Anschlag	BSI-IT-GS-G 0.5	
	GF-I-18	Abhören von Leitungen	BSI-IT-GS-G 0.5	
	GF-I-19	Manipulation an Leitungen (inkl. Stromleitungen)	BSI-IT-GS-G 0.5	

Gefahrenfeld-I baulich/physische Gefahren & umweltbezogene Gefahren				
Subkategorie	Nr.	Gefahren	Referenz	Bemerkung
	GF-I-20	Unberechtigte IT-Nutzung	BSI-IT-GS-G 0.5	
	GF-I-21	Missbrauch von Fernwartungszugängen	BSI-IT-GS-G 0.5	
	GF-I-22	Vertraulichkeitsverlust von in TK-Anlagen gespeicherten Daten	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	
	GF-I-25	Missbrauch von Leistungsmerkmalen von TK-Anlagen	BSI-IT-GS-G 0.5	
	GF-I-26	Unerkannter unbefugter Zutritt		
	GF-I-27	Gefahr von technischen Defiziten bei Alarmanlagen		
	GF-I-28	Gefahr von Objektschutzverletzungen durch Baustellenbetrieb		
Gefahren, die durch Elementarereignisse entstehen können	GF-I-29	Gefahr von schwerem Schneefall und Eis	ENISA-GL-4.1.1	
	GF-I-30	Gefahr von Starkwind und Sturm	ENISA-GL-4.1.2	
	GF-I-31	Gefahr von Überflutungen und Überschwemmungen	ENISA-GL-4.1.3	
	GF-I-32	Gefahr eines Erdbebens und bauliche Unzulänglichkeiten (Eurocode 8)	ENISA-GL-4.1.4	
	GF-I-33	Gefahr eines Waldbrandes	ENISA-GL-4.1.5	
	GF-I-34	Naturkatastrophen	BSI-IT-GS-G 0.5	
	GF-I-35	Katastrophen im Umfeld	BSI-IT-GS-G 0.5	
	GF-I-36	Hochwasser- Unterbrechung von bodengebundenen Kommunikationskanälen (Unterbrechung von Kommunikation)		
	GF-I-37	Starkniederschlagereignisse-Unterbrechung der Kommunikation		
	GF-I-38	Gefahr eines Sonnensturms		
	GF-I-39	Gefahr einer Lawine/Mure/Hangrutschung		
Technische Gefahren	GF-I-40	Gefahr eines Brandes	ENISA-GL-4.1.6 ISO-27001-6.2	

Gefahrenfeld-I baulich/physische Gefahren & umweltbezogene Gefahren				
Subkategorie	Nr.	Gefahren	Referenz	Bemerkung
	GF-I-41	Gefahr von elektromagnetischen Interferenzen	ENISA-GL-4.1.8 ITU-T-REC-X-6.3.2.1	
	GF-I-42	Gefahr von Spannungsschwankungen	ENISA-GL-4.1.17 ISO-27001-6.3	
	GF-I-43	Gefahr eines Kühlungsausfalls/Klimaanlagenausfalls/Ausfalls HKL	ENISA-GL-4.1.18	
	GF-I-44	Gefahr eines Hardwareausfalls	ENISA-GL-4.1.19	
	GF-I-45	Gefahr einer inkompatiblen Hardwareänderung/ Updates	ENISA-GL-4.1.22	
	GF-I-46	Gefahr eines Treibstoffmangels	ENISA-GL-4.1.25	
	GF-I-47	Gefahr von Infrastrukturschäden/-versagen		
	GF-I-48	Gefahr logischer Fehler von redundanten gleichen Systemen		
	GF-I-49	Rohrbrüche (Wasserleitungen)		
	GF-I-50	Fehler in Löschanlagen (Nichtauslösung und Verlegeprobleme)		
	GF-I-51	Wasserführende Rohrleitungen in der Nähe von sensiblen Anlagen		
	GF-I-52	Ausfall von Alarm/Zutrittskontrollsystemen		
	GF-I-53	Gefahr eines Verkehrsunfalls mit Beschädigung von Infrastruktur (auch Brand/Explosion)		
	GF-I-54	Gefahr der Zerstörung durch Einwirkung von Hochspannung		
	GF-I-55	Gefahr von Infrastruktur-/Leitungsschäden durch Manipulation Dritter		
	GF-I-56	Vektorenproblem		
	GF-I-57	Fehler USV/Notstromanlage		
	GF-I-58	Gefahr von Großbaustellen/Baustellen in unmittelbarer Nähe zu sensiblen Infrastrukturen inkl. Fliegerbombenfund		
	GF-I-59	Gebäudesperren		
	GF-I-60	Nicht normgerechte Verlegung von Infrastrukturen		
	GF-I-61	Vorsätzliche Störungen (SDR, Jamming)		

Gefahrenfeld-II: Gefahren durch HR und org. Defizite

Gefahrenfeld-II Gefahren durch HR und org. Defizite				
Subkategorie	Nr.	Gefahren	Referenz	Bemerkung
Gefahren durch ISMS-Defizite	GF-II-01	User errors, Gefahren durch menschliche Fehlleistungen	ITU-T-REC-X-6.3.2.2	
	GF-II-02	Policy or procedure flaw	ENISA-GL-4.1.26	
	GF-II-03	Gefahr von Defiziten bei der ISMS internen Organisation	ISO-27001-1.1	
	GF-II-04	Sicherheitssensibilisierung und -schulung	ISO-27001-1.3	
	GF-II-05	Gefahr durch ungewollte Offenlegung von schützenswerter Information durch Defizite bei Information classification (durchgehend)	ISO-27002-8.2	
	GF-II-06	Offenlegung schützenswerter Informationen	BSI-IT-GS-G 0.5	
	GF-II-07	Media handling insbesondere Entsorgung/ Vernichtung/Weiternutzung	ISO-27002-8.3	
	GF-II-08	Gefahr durch mangelnde IT-Sec Awareness User responsibilities	ISO-27002-9.3	
	GF-II-09	System and application access control	ISO-27002-9.4	
	GF-II-10	Ungeeignete Entsorgung der Datenträger und Dokumente	BSI-IT-GS-G 0.5	
	GF-II-11	Unzureichende Sensibilisierung für Informationssicherheit (inkl. Vorbildfunktion des Managements)	BSI-IT-GS-G 0.5	
	GF-II-12	Unzureichender Schutz der Kommunikation bei Druckern und Multifunktionsgeräten	BSI-IT-GS-G 0.5	
	GF-II-13	Unberechtigte Sammlung personenbezogener Daten	BSI-IT-GS-G 0.5	
	GF-II-14	Gefälschte Zertifikate	BSI-IT-GS-G 0.5	
	GF-II-15	Gefahr eines menschl. Versagens, das die Abschaltung von x- tausend Kunden zur Folge hat		
	GF-II-16	Unzureichende HR-Ressourcen (Qualität und Quantität inkl. Wissenstransfer)		
	GF-II-17	Gefahren durch Zutrittsregelungen		
Gefahren durch Zusammenarbeit mit	GF-II-18	Gefahr von Defiziten bei der Zusammenarbeit mit externen Dritten	ISO-27001-1.2	
	GF-II-19	Gefahren durch Mobile Computing und Telearbeit sowie PDAs inkl. Wartungsinstrumente/ Einsatz	ISO-27001-1.3	

Gefahrenfeld-II Gefahren durch HR und org. Defizite				
Subkategorie	Nr.	Gefahren	Referenz	Bemerkung
externen Dritten		unsicherer Betriebsmittel durch Mitarbeiter (BYOD)		
	GF-II-20	Fehlendes Audit-Regime		
	GF-II-21	Outsourcing sicherheitsrelevanter Services/Dienstleistungen		
Personal-Security	GF-II-22	Gefahren vor dem Beschäftigungsverhältnis	ISO-27002-7.1	
	GF-II-23	Gefahren während dem Beschäftigungsverhältnis	ISO-27002-7.2	
	GF-II-24	Gefahren bei Ende und Wechsel des Beschäftigungsverhältnisses	ISO-27002-7.3	
	GF-II-25	Missbrauch von Leistungsmerkmalen von TK-Anlagen	ISO-27001-1.1	
	GF-II-26	Social Engineering	BSI-IT-GS-G 0.5	
	GF-II-27	Manipulation durch Familienangehörige und Besucher	BSI-IT-GS-G 0.5	
	GF-II-28	Mängel bei Beweisbarkeit Nachvollziehbarkeit von "Schadaktionen"		
	GF-II-29	Ausfall und Verlust von Schlüsselpersonal/Personalredundanzen		
	GF-II-30	Bedrohung von Mitarbeitern inkl. VIPs		
	GF-II-31	Gefahr von Clustering von Mitarbeitern (ges. GF in einem Flugzeug u.dgl.)		
	GF-II-32	Burnout/Überforderung von Mitarbeitern		
	GF-II-33	Gefahren durch Verhalten auf Dienstreisen		
Asset management	GF-II-34	Defizite bei Responsibility for assets	ISO-27002-8.1	
	GF-II-35	Fehlerhafte Outsourcing-Strategie	BSI-IT-GS-G 0.5	
	GF-II-36	Unzureichende Regelungen für das Ende des Outsourcing-Vorhabens	BSI-IT-GS-G 0.5	
	GF-II-37	Gefahren durch M&A		
	GF-II-38	Nutzung von Statussymbolen (ungeschützte Mobile Devices etc.)		
	GF-II-39	Weiterreichung von Security-Verantwortung an Dritte/Regelung von Security-Verantwortlichkeiten		
	GF-II-40	Soziale Inkompatibilitäten unter Mitarbeitern		

Gefahrenfeld-II Gefahren durch HR und org. Defizite				
Subkategorie	Nr.	Gefahren	Referenz	Bemerkung
	GF-II-41	Gefahr durch unzureichende/veraltete Dokumentation		
	GF-II-42	Gefahr der Nichtverfügbarkeit von Entscheidungsträgern oder Zeichnungsberechtigten		
	GF-II-43	Probleme durch Know-how-Defizit oder mangelnde Schulungen		
	GF-II-44	Obsoleszenz-Review (nicht mehr benötigte Inhalte nach Projektende)		
	GF-II-45	Fehlende Sanktionierung von Sicherheitsverletzungen		
	GF-II-46	Fehlende Prozesse zur Erteilung von Zugangsberechtigungen		
	GF-II-47	Fehlendes Change-Management		
	GF-II-48	Auftretende Probleme durch Kostenreduktion		
	GF-II-49	Gefahr bei vermeintlich verschlüsselter Kommunikation und/oder Daten		
	GF-II-50	U-Boot IT (Unkoordinierte Eigen- und Fremdentwicklungen mit Gefahr von Sicherheitslücken)		
	GF-II-51	Mangelnde Verantwortlichkeit des Managements bei Security-Themen		Budget-hoheit!

Gefahrenfeld-III: Kryptographie/Software/Protokolle

Gefahrenfeld-III Kryptographie/Software/Protokolle				
Subkategorie	Nr.	Gefahren	Referenz	Bemerkung
Umsetzungen / Implementierungen	GF-III-01	Cryptographic controls, Schwächen in den Algorithmen	ISO-27002-10.1	
	GF-III-02	Manipulation oder Defizite bei Hard- oder Software	BSI-IT-GS-G 0.5	
	GF-III-03	Software bug	ENISA-GL-4.1.20	
	GF-III-04	Fortführender Fehler durch Vererbung in den Libraries, Reuse of Code		
	GF-III-05	Faulty Software Change/Update	ENISA-GL-4.1.23	
	GF-III-06	Gefahr bei Kombination aus Hard- und Software		
	GF-III-07	Fehlerhafte Zeitsynchronisation	BSI-IT-GS-G 0.5	

	GF-III-08	Gefahr, der absichtlich eingebaute Schwachstellen bei Normen/ Standards (zu geringe Entropie etc.)		
	GF-III-09	Fehlbedienung oder falsche Implementierung von Kryptomodulen	BSI-IT-GS-G 0.5	
	GF-III-10	Unsichere Konfiguration der VPN-Clients für den Fernzugriff	BSI-IT-GS-G 0.5	
	GF-III-11	Fortgesetzter Einsatz unsicherer kryptographische Algorithmen	BSI-IT-GS-G 0.5	
	GF-III-12	Veralten von Kryptoverfahren (Upgrades/Updates) – Quantencomputer	BSI-IT-GS-G 0.5	
	GF-III-13	Praxisferne Implementierung von Sicherheitsverfahren (Gefahr der Umgehung)		
	GF-III-14	Defizite im Zertifikatsmanagement		
	GF-III-15	Defizite bei der Entwicklung von Software		
	GF-III-16	Kompromittierte externe CAs		
	GF-III-17	Defizite in Default Trust-Stores		
	GF-III-18	Diebstahl von Schlüsselmaterial		
	GF-III-19	Unzureichender Schutz von Softwarebibliotheken		
	GF-III-20	Defizite bei hardwarenahen Sicherheitsmechanismen (UEFI, HDs, etc.)		
	GF-III-21	Verlust von Schlüsseln (Auch Zerstörung)		
	GF-III-22	Unverschlüsselte Metadaten		
	GF-III-23	Probleme bei der Analyse von end to end-verschlüsselten Datenströmen		
	GF-III-24	Umgang mit Zertifikatsfehlern		
	GF-III-25	Missbrauch von Leistungs-merkmalen von TK-Anlagen		
	GF-III-26	Unangepasste Aufbewahrung von Schlüsselmaterial		
	GF-III-27	Einsatz von weak keys		
	GF-III-28	Nichtanwendung von Krypto		
	GF-III-29	Einsatz von nicht allgemein anerkannten kryptographischen Verfahren		
	GF-III-30	Provisionierung von Kryptographie (SIM-Karten)		

Gefahrenfeld IV: Zugriffskontrolle/Berechtigungssysteme & Schlüssel-Passwortverwaltung

Gefahrenfeld IV Zugriffskontrolle/Berechtigungssysteme & Schlüssel-Passwortverwaltung				
Subkategorie	Nr.	Gefahren	Referenz	Bemerkung
	GF-IV-01	Gefahr von User Errors	ITU-T-REC-X-6.3.2.2	
	GF-IV-02	Weak access control mechanisms	ITU-T-REC-X-6.3.2.3	
	GF-IV-03	Badly configured network routers, gateways or firewalls	ITU-T-REC-X-6.3.2.3	
	GF-IV-04	Lack of user Authentification Methods	ITU-T-REC-X-6.3.2.3	
	GF-IV-05	Defizite bei User access management	ISO-27002-9.2	
	GF-IV-06	Gefahr von Defiziten bei Business requirements of access control	ISO-27002-9.1	
	GF-IV-07	Gefahr von Defiziten bei der Zugriffskontrollpolitik	ISO-27001-1.1	
	GF-IV-08	Gefahr von Defiziten bei der Benutzerverwaltung	ISO-27001-1.2	
	GF-IV-09	Mangelnde Security Awareness bei Access Control	ISO-27001-1.3	
	GF-IV-10	Mangelnde Securityregelungen bei Fernzugriffenn	ISO-27001-1.4	
	GF-IV-11	Fehlende oder unzureichende Schulung der Telearbeiter	BSI-IT-GS-G 0.5	
	GF-IV-12	Mangelhafte Einbindung des Telearbeiters in den Informationsfluss	BSI-IT-GS-G 0.5	
	GF-IV-13	Mangelnde Securityregelungen bei Zugriff auf Betriebssysteme	ISO-27001-1.5	
	GF-IV-14	Mangelnde Securityregelungen bei Zugriff auf Anwendungen und Informationen	ISO-27001-1.6	
	GF-IV-15	Unerkannte unerlaubte Ausübung von Rechten	BSI-IT-GS-G 0.5	
	GF-IV-16	Ungeregelte Weitergabe von Datenträgern	BSI-IT-GS-G 0.5	
	GF-IV-17	Unzureichendes Schlüssel-management bei Verschlüsselung	BSI-IT-GS-G 0.5	
	GF-IV-18	Mangelhafte Organisation des Wechsels zwischen den Benutzern	BSI-IT-GS-G 0.5	
	GF-IV-19	Fehlende Auswertung von Protokolldaten	BSI-IT-GS-G 0.5	
	GF-IV-20	Ungeeignete Einschränkung der Benutzerumgebung	BSI-IT-GS-G 0.5	

Gefahrenfeld IV Zugriffskontrolle/Berechtigungssysteme & Schlüssel-Passwortverwaltung				
Subkategorie	Nr.	Gefahren	Referenz	Bemerkung
	GF-IV-21	Unkontrollierter Aufbau von Kommunikationsverbindungen	BSI-IT-GS-G 0.5	
	GF-IV-22	Unzureichende Identifikationsprüfung von Kommunikationspartnern	BSI-IT-GS-G 0.5	
	GF-IV-23	Gefährdung bei Wartungs-/ Administrierungsarbeiten	BSI-IT-GS-G 0.5	
	GF-IV-24	Gefährdung bei Wartungsarbeiten durch externes Personal	BSI-IT-GS-G 0.5	
	GF-IV-25	Missbrauch von Leistungs-merkmalen von TK-Anlagen	BSI-IT-GS-G 0.5	
	GF-IV-26	Gefahr, dass Unbefugte Zugang zu nicht privilegierten Remote-Access-Accounts, LAN-Accounts mit Privilegien oder Remote- Access-LAN- Accounts mit Privilegien erhalten		
	GF-IV-27	Gefahr, dass während der Authentifizierung Informationen an unbefugte Dritte zurückgegeben werden (Bsp. Maskieren der Passwortinformationen)		
	GF-IV-28	Gefahr der Kolokation		

Gefahrenfeld-V: Operations Security (OS/Software und Datenbank)

Gefahrenfeld-V Operations Security (OS/Software und Datenbank)				
Subkategorie	Nr.	Gefahren	Referenz	Bemerkung
Vertraulichkeit	GF-V-01	Gefahr des Abhörens elektromagnetischer Strahlung	ITU-T-REC-X-6.3.2.1	
	GF-V-02	Eavesdropping	ITU-T-REC-X-6.3.2.1	
	GF-V-03	Misrouting/rerouting of Messages	ITU-T-REC-X-6.3.2.1	
	GF-V-04	Software Failure	ITU-T-REC-X-6.3.2.1	
	GF-V-05	Theft (physisch und logisch)	ITU-T-REC-X-6.3.2.1	
	GF-V-06	Unauthorized access to computers, data, services and applications	ITU-T-REC-X-6.3.2.1	
	GF-V-07	Unauthorized access to storage media	ITU-T-REC-X-6.3.2.1	
	GF-V-08	Manipulation von Hard- oder Software	BSI-IT-GS-G 0.5	
	GF-V-09	Backup	ISO-27002-12.3	
	GF-V-10	Dateilose Infektion		
	GF-V-11	Logging and monitoring(Datenhaltung)	ISO-27002-12.4	
	GF-V-12	Unauthorized access to storage media	ITU-T-REC-X-6.3.2.3	
	GF-V-13	Client-seitige Angriffe		
Integrität	GF-V-14	Malicious Code	ITU-T-REC-X-6.3.2.1	
	GF-V-15	Masquerading of user identity/Fälschung von Adressierungselementen (Falsche Telefonnummern, Fax-Nummern, SMS-Absender, E-Mailadressen)	ITU-T-REC-X-6.3.2.1	
	GF-V-16	Unauthorized modification of information	ITU-T-REC-X-6.3.2.2	
	GF-V-17	Deterioration of storage media	ITU-T-REC-X-6.3.2.2	
	GF-V-18	Malicious code	ITU-T-REC-X-6.3.2.2	
	GF-V-19	Masquerading of user identity	ITU-T-REC-X-6.3.2.2	
	GF-V-20	Misrouting/rerouting of messages	ITU-T-REC-X-6.3.2.2	

Gefahrenfeld-V Operations Security (OS/Software und Datenbank)				
Subkategorie	Nr.	Gefahren	Referenz	Bemerkung
	GF-V-21	Repudiation	ITU-T-REC-X-6.3.2.2	
	GF-V-22	Software failures and vulnerabilities	ITU-T-REC-X-6.3.2.2	
	GF-V-23	Supply failures (power, air conditioning)	ITU-T-REC-X-6.3.2.2	
	GF-V-24	Technical failures and vulnerabilities	ITU-T-REC-X-6.3.2.2	
	GF-V-25	Missbrauch von Leistungs-merkmalen von TK-Anlagen	ITU-T-REC-X-6.3.2.2	
	GF-V-26	Unauthorized access to computers, data, services and applications	ITU-T-REC-X-6.3.2.2	
	GF-V-27	Use of unauthorized programs and data	ITU-T-REC-X-6.3.2.2	
	GF-V-28	User errors	ITU-T-REC-X-6.3.2.2	
	GF-V-29	Manipulation von Hard- oder Software	BSI-IT-GS-G 0.5	
	GF-V-30	Inkompatibilität zwischen fremder und eigener IT	BSI-IT-GS-G 0.5	
	GF-V-31	Fehlerhafte Konfiguration eines DNS-Servers	BSI-IT-GS-G 0.5	
	GF-V-32	Man-in-the-Middle-Angriff	BSI-IT-GS-G 0.5	
	GF-V-33	DNS-Flooding - Denial-of-Service	BSI-IT-GS-G 0.5	
	GF-V-34	DNS-Hijacking	BSI-IT-GS-G 0.5	
	GF-V-35	DNS-Amplification Angriff	BSI-IT-GS-G 0.5	
	GF-V-36	DNS Information Leakage	BSI-IT-GS-G 0.5	
	GF-V-37	Ausnutzen dynamischer DNS-Updates	BSI-IT-GS-G 0.5	
Verfügbarkeit	GF-V-38	Software bug	ENISA-GL-4.1.20	
	GF-V-39	Fortführender Fehler durch Vererbung in den Libraries		
	GF-V-40	Faulty Software Change/Update	ENISA-GL-4.1.23	
	GF-V-41	Gefahr von schlecht aufeinander abgestimmter Kombination aus Hard- und Software		
	GF-V-43	Operational procedures and responsibilities	ISO-27002-12.1	

Gefahrenfeld-V Operations Security (OS/Software und Datenbank)				
Subkategorie	Nr.	Gefahren	Referenz	Bemerkung
	GF-V-44	Missing Protection from malware	ISO-27002-12.2	
	GF-V-47	Control of operational software	ISO-27002-12.5	
	GF-V-48	Technical vulnerability management	ISO-27002-12.6	
	GF-V-49	Information systems audit considerations	ISO-27002-12.7	
	GF-V-50	DoS-Attack	ENISA-GL-4.1.9	
	GF-V-51	Network traffic hijack	ENISA-GL-4.1.10	
	GF-V-52	Malware and viruses	ENISA-GL-4.1.11	
	GF-V-53	Advanced persistent threat	ENISA-GL-4.1.12	
	GF-V-54	Overload, technisch	ENISA-GL-4.1.24	
	GF-V-55	Gefahr eines DoS-Angriffs		
	GF-V-56	Destructive attacks	ITU-T-REC-X-6.3.2.3	
	GF-V-57	Denial of service attacks	ITU-T-REC-X-6.3.2.3	
	GF-V-58	Deterioration of storage media	ITU-T-REC-X-6.3.2.3	
	GF-V-59	Failure of communication equipment and services	ITU-T-REC-X-6.3.2.3	
	GF-V-60	Physical damage due to fire, flood, explosions or earthquakes	ITU-T-REC-X-6.3.2.3	siehe GF I
	GF-V-61	Maintenance errors	ITU-T-REC-X-6.3.2.3	
	GF-V-62	Malicious code	ITU-T-REC-X-6.3.2.3	
	GF-V-63	Misrouting or rerouting of messages	ITU-T-REC-X-6.3.2.3	
	GF-V-64	Misuse of resources	ITU-T-REC-X-6.3.2.3	
	GF-V-65	Software failures and vulnerabilities	ITU-T-REC-X-6.3.2.3	
	GF-V-66	Supply failure (power, air conditioning)	ITU-T-REC-X-6.3.2.3	
	GF-V-67	Failures of back-up systems	ITU-T-REC-X-6.3.2.3	
	GF-V-68	Technical failures and vulnerabilities	ITU-T-REC-X-6.3.2.3	

Gefahrenfeld-V Operations Security (OS/Software und Datenbank)				
Subkategorie	Nr.	Gefahren	Referenz	Bemerkung
	GF-V-69	Theft (physisch)	ITU-T-REC-X-6.3.2.3	
	GF-V-70	Masquerading of user identity	ITU-T-REC-X-6.3.2.3	
	GF-V-71	Traffic overloading	ITU-T-REC-X-6.3.2.3	
	GF-V-72	Transmission errors	ITU-T-REC-X-6.3.2.3	
	GF-V-73	Unauthorized access to computers, data, services and applications	ITU-T-REC-X-6.3.2.3	
	GF-V-74	Use of unauthorized programs and data	ITU-T-REC-X-6.3.2.3	
	GF-V-77	User errors and mistakes	ITU-T-REC-X-6.3.2.3	
	GF-V-78	Outdated software patches	ITU-T-REC-X-6.3.2.3	Kontext zu 62
	GF-V-79	Gefahr logischer Fehler von redundanten gleichen Systemen		
	GF-V-80	Ausfall oder Störung von Kommunikationsnetzen vorgelagerter oder nachgelagerter Betreiber	BSI-IT-GS-G 0.5	
	GF-V-81	Ausfall oder Störung von abhängigen Dienstleistern	BSI-IT-GS-G 0.5	
	GF-V-82	Ausfall von Geräten oder Systemen	BSI-IT-GS-G 0.5	
	GF-V-83	Fehlfunktion von Geräten oder Systemen	BSI-IT-GS-G 0.5	
	GF-V-84	Ressourcenmangel	BSI-IT-GS-G 0.5	
	GF-V-85	Fehlende oder unzureichende Wartung	BSI-IT-GS-G 0.5	
	GF-V-86	Fehlende oder unzureichende Planung des Speichersystems	BSI-IT-GS-G 0.5	
	GF-V-87	Mangelhafte Organisation bei Versionswechsel und Migration von Datenbanken	BSI-IT-GS-G 0.5	
	GF-V-88	Fehlerhafte Zeitsynchronisation	BSI-IT-GS-G 0.5	
	GF-V-89	Ausfall von Monitoringsystemen		
	GF-V-90	Zero Day-Exploits		
	GF-V-91	SQL-Injection		
	GF-V-92	Ungewollte öffentliche Erreichbarkeit von Diensten aus dem Internet		
	GF-V-93	Vortäuschung/Social Engineering		
	GF-V-94	Sicherheit von Steuerungsanlagen		
	GF-V-95	Sicherheit von Nebenstellanlagen		

Gefahrenfeld-V Operations Security (OS/Software und Datenbank)				
Subkategorie	Nr.	Gefahren	Referenz	Bemerkung
	GF-V-96	Zugriff von Testsystemen auf Produktivdaten und vice versa		
	GF-V-97	Nicht funktionierende Restores		
	GF-V-98	Fehlende Vertraulichkeit von Dienstleistern		
	GF-V-99	Unvollständige Testbarkeit von Redundanzen		
	GF-V-100	Ausgelaufene Lizenzierung		

Gefahrenfeld-VI: Communications Security

Gefahrenfeld-VI Communications Security				
Subkategorie	Nr.	Gefahren	Referenz	Bemerkung
	GF-VI-01	Kein/Mangelhaftes Network security management	ISO-27002-13.1	
	GF-VI-02	Keine/mangelhafte Abstimmung/ Koordination im Netzwerkbereich	ISO-27002-13.2	
	GF-VI-03	Misrouting/rerouting of Messages	ITU-T-REC-X-6.3.2.1	
	GF-VI-04	Fehler im BGP-Protokoll etc./ Fehlende Spezifikation von Protokollen (IPSec)		
	GF-VI-05	Miskonfiguration/Fehlkonfiguration		
	GF-VI-06	Fehlplanung oder fehlende Anpassung der Network Security	BSI-IT-GS-G 0.5	
	GF-VI-07	Manipulation von Hard- oder Software (Auch Antennentechnologie)	BSI-IT-GS-G 0.5	
	GF-VI-08	Unsicherer Fernzugriff	BSI-IT-GS-G 0.5	
	GF-VI-09	Probleme bei der Authentifizierung (abgelaufene Zertifikate etc.)		
	GF-VI-10	Man in the middle-Angriffe		
	GF-VI-11	Gefahren durch unverschlüsselte WLANs		
	GF-VI-12	Offen zugängliche Netzwerkbuchsen (NAC-Security) - offene und aktivierte Ports		
	GF-VI-13	Inkompatibilitäten/Gefahren durch Network-Sharing - Netzwerkkomponenten		
	GF-VI-14	Software bug	ENISA-GL-4.1.20	
Architektur	GF-VI-15	Fortführender Fehler durch Vererbung in den Libraries		

Gefahrenfeld-VI Communications Security				
Subkategorie	Nr.	Gefahren	Referenz	Bemerkung
	GF-VI-16	Faulty Software Change/Update	ENISA-GL-4.1.23	
	GF-VI-17	Gefahr von schlecht aufeinander abgestimmter Kombination aus Hard- und Software		
	GF-VI-18	Design error, Design ist nicht mehr für die Use Cases adäquat	ENISA-GL-4.1.21	
	GF-VI-19	Gefahr, dass konzeptionelle Schwachstellen bei Segmentierungen (Trennung von control plain und user plain)		
	GF-VI-20	Mögliche Gefahren für die SCADA-Netze SS7 etc.		
	GF-VI-21	Gefahr, dass in abgeschotteten LAN/Netzwerk/SCADAsystemen Angriffe durchgeführt werden können (DoS)		
	GF-VI-22	Gefahr logischer Fehler von redundanten gleichen Systemen		
	GF-VI-23	Inkompatible aktive und passive Netzkomponenten	BSI-IT-GS-G 0.5	
	GF-VI-24	Betreiben von nicht angemeldeten/autorisierten Komponenten (NAC-Security, auch Software)	BSI-IT-GS-G 0.5	
	GF-VI-25	Missbrauch von Leistungs-merkmalen von TK-Anlagen	BSI-IT-GS-G 0.5	
	GF-VI-26	Inkompatibilität zwischen fremder und eigener IT	BSI-IT-GS-G 0.5	
	GF-VI-27	Fehlerhafte Zeitsynchronisation	BSI-IT-GS-G 0.5	
	GF-VI-28	Leitungsbeeinträchtigung durch Umfeldfaktoren	BSI-IT-GS-G 0.5	
	GF-VI-29	Übersprechen/Interferenzen = Betriebsstörung	BSI-IT-GS-G 0.5	
	GF-VI-30	Unsicher/Keine Default-Einstellungen auf Routern und Switches	BSI-IT-GS-G 0.5	
	GF-VI-31	Unsichere Konfiguration der VPN-Clients für den Fernzugriff	BSI-IT-GS-G 0.5	
	GF-VI-32	Missbrauch von Protokollen	BSI-IT-GS-G 0.5	
	GF-VI-33	Missbrauch der Routing-Protokolle	BSI-IT-GS-G 0.5	
	GF-VI-34	Missbrauch von Netzanalyse-Tools (Replay-Attacks=Man in the middle etc.)	BSI-IT-GS-G 0.5	

Gefahrenfeld-VI Communications Security				
Subkategorie	Nr.	Gefahren	Referenz	Bemerkung
	GF-VI-35	Gefahr, dass Equipment ohne organisatorische eineindeutige Identifikation im LAN/Netzwerk/ Fernwirksystem/Netzleitsystem/ Prozessleitsystem in Betrieb genommen werden können (Organisatorisch - MAC, oder Maschinenzertifikate)		
	GF-VI-36	Gefahr, dass die Integrität eingeführter, abgesicherter Kommunikation kompromittiert wird.		
	GF-VI-37	Gefahr, dass die Vertraulichkeit eingeführter, abgesicherter Kommunikation kompromittiert wird		
	GF-VI-38	Gefahr, dass ungeprüfte Software/ Firmware/Code im produktiven Betrieb eingesetzt wird und damit die funktionale Sicherheit oder Security-relevante Funktionen "gestört" werden können		
	GF-VI-39	Gefahr, dass eine (konzeptionelle) Schwäche in der funktionalen Sicherheit ein vorgesehenes Security-Feature kompromittiert		
	GF-VI-40	Gefahr von nicht erkannten Serienfehlern ==> schlimmer bei homogener Infrastruktur		
Diskussion der Gefahren bei OSI-Layer 1-5	GF-VI-41	Gefahren, die auf OSI-Layer 1 wirken		
	GF-VI-42	Gefahren, die auf OSI-Layer 2 wirken		
	GF-VI-43	Gefahren, die auf OSI-Layer 3 wirken		
	GF-VI-44	Gefahren, die auf OSI-Layer 4 wirken		
	GF-VI-45	Gefahren, die auf OSI-Layer 5 wirken		
	GF-VI-46	Gebührenbetrug	BSI-IT-GS-G 0.5	
	GF-VI-47	Unzureichende Dokumentation der Topologie (Unzureichender Informationsaustausch zwischen Unternehmen)		

Gefahrenfeld-VI Communications Security				
Subkategorie	Nr.	Gefahren	Referenz	Bemerkung
	GF-VI-48	Fehler oder unzureichende Implementierung von globalen Protokollen		
	GF-VI-49	Fehler oder unzureichende Implementierung von internen Protokollen		
	GF-VI-50	Fehler oder unzureichende Implementierung bei Kunden		
	GF-VI-51	Missbrauch von BGP		
	GF-VI-52	Missbrauch von SS7		
	GF-VI-53	Missbrauch von SCADA/Fernwirktechnik/Leittechnik		
	GF-VI-54	Legacy Support		
	GF-VI-55	Verhindern von Adress-spoofing von eigenen Kunden BCP38/CLI (gilt auch für Telefonie) - Eigenkunden/Fremdkunden		
	GF-VI-56	Mangelnde Sichtbarkeit über Vorgänge im Netz (Angriffserkennung/mangelhafte oder fehlende Anomalieerkennung)		
	GF-VI-57	Fehlende Redundanz bei Managementsystemen		
	GF-VI-58	Fehlende physische Redundanz		
	GF-VI-59	Zu hohe Sendeleistung von WLAN-Routern in Verbindung mit nicht gesicherten WLANs		
	GF-VI-60	Mangelnde CPE-Sicherheit		
	GF-VI-61	Wire-Tapping inkl. Funküberwachung		
	GF-VI-62	Intentionale physische Unterbrechung von Kommunikationskanälen		
	GF-VI-63	Störung von Richtfunk		
	GF-VI-64	Unbezahlte Rechnungen		
	GF-VI-65	Gefahr fehlerhafter Implementierung bei Netzübergängen		
	GF-VI-66	Gefahr der Betriebsstörung bei Security-Tests von Teilsystemen		
	GF-VI-67	Gefahr von Störungen im/bei intern benutzten Protokollen wie MPLS etc.		
	GF-VI-68	Gefahr von Missbrauch/Störung in Protokollen, wo mit Kunden		

Gefahrenfeld-VI Communications Security				
Subkategorie	Nr.	Gefahren	Referenz	Bemerkung
		gesprochen wird (v.a. auf Routing-Ebene)		
	GF-VI-69	Gefahr durch veraltete Protokolle		
	GF-VI-70	Ausgelaufene Lizenzierung		
	GF-VI-71	Einsatz von nicht getesteten Netzwerkkomponenten (bezogen auf Security und funktionale Sicherheit)		
	GF-VI-72	Gefahr von Breaches zwischen Netzwerksegmenten aus organisatorischen Gründen		
	GF-VI-73	Unerkannte Einfallstore ins Management		
	GF-VI-74	Manipulation von Hard- oder Software im Endgerätebereich		

Gefahrenfeld-VII: System Aquisition & Development & Maintenance & Decommissioning

Gefahrenfeld-VII System Aquisition & Development & Maintenance & Decommissioning				
Subkategorie	Nr.	Gefahren	Referenz	Bemerkung
	GF-VII-01	Defizite bei der Security Anforderungen an Systeme	ISO-27002-14.1	
	GF-VII-02	Defizite bei Security in Development and Support Process (Fehlende Programmierrichtlinien)	ISO-27002-14.2	
	GF-VII-03	Defizite bei Test Regimen and Test Data z.B. keine 61508ff oder V-Modell	ISO-27002-14.3	
	GF-VII-04	Ausfall oder Störung von abhängigen Dienstleistern	BSI-IT-GS-G 0.5	
	GF-VII-05	fehlendes oder unzureichendes Test- und Freigabeverfahren (inkl. mangelhafte Integrationstests)	BSI-IT-GS-G 0.5	
	GF-VII-06	fehlerhafte oder unzureichende Dokumentation	BSI-IT-GS-G 0.5	
	GF-VII-07	mangelnde oder falsche Berücksichtigung von Geschäftsprozessen beim Patch- und Änderungsmanagement	BSI-IT-GS-G 0.5	
	GF-VII-08	mangelhaft festgelegte Verantwortlichkeiten beim Patch- und Änderungsmanagement	BSI-IT-GS-G 0.5	insgesamt zu sehen!
	GF-VII-09	Unzureichende Ressourcen beim Patch- und Änderungsmanagement	BSI-IT-GS-G 0.5	

Gefahrenfeld-VII System Aquisition & Development & Maintenance & Decommissioning				
Subkategorie	Nr.	Gefahren	Referenz	Bemerkung
	GF-VII-10	Mangelhafte Kommunikation beim Patch- und Änderungsmanagement	BSI-IT-GS-G 0.5	
	GF-VII-11	Fehlende Übersicht über den Informationsverbund	BSI-IT-GS-G 0.5	
	GF-VII-12	Fehlende und unzureichende Planung bei der Verteilung von Patches und Änderungen	BSI-IT-GS-G 0.5	
	GF-VII-13	Mangelhafte Wiederherstellungs-optionen beim Patch- und Änderungsmanagement	BSI-IT-GS-G 0.5	
	GF-VII-14	Mangelhafte Berücksichtigung von mobilen Endgeräten beim Patch- und Änderungsmanagement	BSI-IT-GS-G 0.5	
	GF-VII-15	Unzureichendes Notfallvorsorgekonzept für das Patch- und Änderungs-management	BSI-IT-GS-G 0.5	
	GF-VII-16	Fehlbedienung von Kryptomodulen	BSI-IT-GS-G 0.5	
	GF-VII-17	Gefährdung bei Wartungs-/ Administrierungsarbeiten	BSI-IT-GS-G 0.5	
	GF-VII-18	Gefährdung bei Wartungsarbeiten durch externes Personal (durch organisatorische Mängel)	BSI-IT-GS-G 0.5	
	GF-VII-19	Manipulation von Managementparametern bzw. Konfigurationsparametern	BSI-IT-GS-G 0.5	
	GF-VII-20	Gefahr, dass durch eine zunehmende Heterogenität in der IKT-Sicherheitsarchitektur ausnutzbare Schwachstellen, die zur Manipulation mit Schadwirkung ausnutzbar sind, zu spät erkannt werden		
	GF-VII-21	Gefahr von nicht erkannten Safety und Security-Schwachstellen und der lange Nutzungszeitraum		
	GF-VII-22	Gefahr, dass geprüfte Software einen erheblichen funktionalen Fehler aufweist		
	GF-VII-23	Gefahr, dass die Performance der Endgeräte zu gering ist (Kommunikationsbandbreite und Rechenkapazität) auch eine langfristige Perspektive		

Gefahrenfeld-VII System Aquisition & Development & Maintenance & Decommissioning				
Subkategorie	Nr.	Gefahren	Referenz	Bemerkung
	GF-VII-24	Gefahr, dass Auslegungskriterien zu (nicht ausreichend) konservativ beurteilt werden (Planungsfehler!)		
	GF-VII-25	Missbrauch von Leistungsmerkmalen von TK-Anlagen		
	GF-VII-26	Gefahr, dass Änderungen von Strukturen und Designs keinen regelmäßigen hollistischen Betrachtungen unterzogen werden		
	GF-VII-27	Gefahr der fehlenden Awarness im Umgang mit alten Betriebs-systemen und bei Security Themen (intern und extern, auch Lieferanten)		
	GF-VII-28	Gefahr der fehlenden Erfahrung/Schulung im Umgang mit Wartungssoftware		
	GF-VII-29	Gefahr der fehlenden Technologiefolgenabschätzungen		
	GF-VII-30	Gefahr, dass Service und Wartungsgeräte (PDA, Laptops etc) durch unbefugte externe Dritte in Besitz genommen werden und darauf unbemerkt Manipulationen über einen längeren Zeitraum (Wochen - Monate) vornehmen können		
	GF-VII-31	Mangelnde Vorhaltung von Ersatzgeräten + Überprüfung		
	GF-VII-32	Out of band-Management		
	GF-VII-33	Mangelnde Rechtevergabe bei Maintenance-Aufgaben		
	GF-VII-34	Sicheres Vernichten/Löschen und Dokumentation von Hard- und Software und Berechtigungen		
	GF-VII-35	Mangelnde Berücksichtigung von Abhängigkeiten (beim Patchen etc.)		
	GF-VII-36	Mangelnde Compliance mit Standards		
	GF-VII-37	Abweichen von vordefinierten Prozessen wegen zu hohem Zeitdruck bei Großprojekten und mangelnde Tests von Interfaces		
	GF-VII-38	IT-Debt		
	GF-VII-39	M&A-Konzernfusionen		

Gefahrenfeld-VII System Aquisition & Development & Maintenance & Decommissioning				
Subkategorie	Nr.	Gefahren	Referenz	Bemerkung
	GF-VII-40	Open Source vs. Proprietäre Lösungen (Stichwort: Managed Source)		

Gefahrenfeld-VIII: Hersteller& Lieferanten Supply Chain

Gefahrenfeld-VIII Hersteller& Lieferanten Supply Chain				
Subkategorie	Nr.	Gefahren	Referenz	Bemerkung
	GF-VIII-01	Information security in supplier relationships (inkl. Datenschutz und Berücksichtigung nationaler Gesetzgebungen)	ISO-27002-15.1	
	GF-VIII-02	Supplier service delivery management	ISO-27002-15.2	
	GF-VIII-03	Ausfall oder Störung von abhängigen Dienstleistern	BSI-IT-GS-G 0.5	
	GF-VIII-04	Ausfall (Konkurs, Produkteinstellung etc.) eines Dienstleisters oder Zulieferers	BSI-IT-GS-G 0.5	
	GF-VIII-05	Unzureichende oder falsche Versorgung mit Verbrauchsgütern	BSI-IT-GS-G 0.5	
	GF-VIII-06	Unzulängliche vertragliche Regelungen mit einem externen Dienstleistern (Sowohl SLA wie auch Haftungsfragen)	BSI-IT-GS-G 0.5	
	GF-VIII-07	Gefahr der fehlende Awarness der Hersteller für IT-Sec ===> (Aufwand/Kosten bei den Herstellern) besser Kollaboration und Kommunikation bei den Betreibern		
	GF-VIII-08	Manipulation von Hard- oder Software	BSI-IT-GS-G 0.5	
	GF-VIII-09	Unzureichende Identifikationsprüfung von Kommunikationspartnern	BSI-IT-GS-G 0.5	
	GF-VIII-10	Manipulation von Managementparametern	BSI-IT-GS-G 0.5	
	GF-VIII-11	Informationen oder Produkte aus unzuverlässiger Quelle	BSI-IT-GS-G 0.5	
	GF-VIII-12	Fortführender Fehler durch Vererbungen in den Libraries, Reuse of Code		
	GF-VIII-13	Hardwaremanipulation		
	GF-VIII-15	Unsichere Kommunikation mit Vendors/Lieferanten		

Gefahrenfeld-VIII Hersteller& Lieferanten Supply Chain				
Subkategorie	Nr.	Gefahren	Referenz	Bemerkung
	GF-VIII-16	Produktfälschungen		
	GF-VIII-17	Serienfehler bei Komponenten		
	GF-VIII-18	Abhängigkeit von (einzelnen) Lieferanten (Awareness)		
	GF-VIII-19	Änderung von Lizenzmodellen		
	GF-VIII-20	Gefahren der Just in time-Logistik inkl. Tests der Supply-Chain		
	GF-VIII-21	Mangelnde Lieferantenaudits		
	GF-VIII-22	Gefahren durch Billigstbieterprinzip/Defizite im Ausschreibungsprozess		
	GF-VIII-23	Defizite im Beschaffungsprozess		
	GF-VIII-24	Nichterfüllung von Wartungsverträgen		

Gefahrenfeld-IX: IM&BCM Kollaboration

Gefahrenfeld-IX IM&BCM Kollaboration				
Subkategorie	Nr.	Gefahren	Referenz	Bemerkung
Harmonisierung der Eskalationsstufen	GF-IX-01	Management of information security incidents and improvements	ISO-27002-16.1	
	GF-IX-02	Information security continuity	ISO-27002-17.1	
	GF-IX-03	Redundancies	ISO-27002-17.2	
	GF-IX-04	User errors	ITU-T-REC-X-6.3.2.2	
	GF-IX-05	Lack of user training	ITU-T-REC-X-6.3.2.3	
	GF-IX-06	Unzureichende Schulung der Mitarbeiter, Dienstleister und Behörden	BSI-IT-GS-G 0.5	
	GF-IX-07	Lack of procedures or badly written procedures	ITU-T-REC-X-6.3.2.3	
	GF-IX-08	Lack of business continuity or contingency arrangements	ITU-T-REC-X-6.3.2.3	
	GF-IX-09	Nicht-Verfügbarkeit des Mobilfunknetzes	BSI-IT-GS-G 0.5	
	GF-IX-10	Ausfall von Sprachverbindungen		

Gefahrenfeld-IX IM&BCM Kollaboration				
Subkategorie	Nr.	Gefahren	Referenz	Bemerkung
	GF-IX-11	Missbrauch sozialer Netzwerke inkl. gezielter Fake News	BSI-IT-GS-G 0.5	
Frühwarnung	GF-IX-12	Ungeeigneter Umgang mit Sicherheitsvorfällen (Vertraulichkeit und KVP)	BSI-IT-GS-G 0.5	
	GF-IX-13	Gefahr des unzureichenden Umgangs bei "near miss" Zuständen (Safurity) ===> Critical Incident Reporting System		
	GF-IX-14	Mögliches Ignorieren von Fehlalarmen und Alarmen der Sicherheitssysteme inkl. mangelndes Tuning		
IM	GF-IX-15	Nicht rechtzeitig erkannte und falsch eingeschätzte Sicherheitsvorfälle	BSI-IT-GS-G 0.5	
	GF-IX-16	Zerstörung von Beweisspuren bei der Behandlung von Sicherheitsvorfällen	BSI-IT-GS-G 0.5	
	GF-IX-17	Unzureichende Identifikationsprüfung von Kommunikationspartnern	BSI-IT-GS-G 0.5	
	GF-IX-18	Fehlende oder falsche Notfallplanung und Eskalationskultur im BCM		
	GF-IX-19	Ausfall von Sensorsystemen		
	GF-IX-20	Gefahr der Nichtverfügbarkeit von Entscheidungsträgern oder Zeichnungsberechtigten		
	GF-IX-21	Gefahr durch fehlende regelmäßige Übungen (Wirksamkeit von Emergency Response-Plans)		
	GF-IX-22	Gefahr durch Ausfälle durch Tests (z.B. Umschaltungen etc.)		
	GF-IX-23	Fehlende Kanalisierung von Störungsmeldungen und Sicherheitshinweisen durch Kunden		Empfehlung!
	GF-IX-24	Mangelhaftes Störungs-, Notfall- und Krisenmanagement inkl. Krisenkommunikation, Aktualisierung der Pläne		Punkte 2, 18 und 20 zusammengefasst!
	GF-IX-25	Missbrauch von Leistungsmerkmalen von TK-Anlagen		
	GF-IX-26	Verfügbarkeit von Hard- und Softwareupdates für das IM sowie externe Hilfe		

Gefahrenfeld-IX IM&BCM Kollaboration				
Subkategorie	Nr.	Gefahren	Referenz	Bemerkung
	GF-IX-27	Unzureichende Kommunikationsressourcen im Notfall inkl. Redundanzen		
	GF-IX-28	Fehlende gemeinsame Sprache zur Ereignisbewältigung z.B. BSI 100-4, ONR 49000ff, ON 2400...		
	GF-IX-29	Fehlende rechtliche Voraussetzungen zum effektiven Datenaustausch zwischen Organisationen im Ereignisfall (z.B. IP-Adressen)		
	GF-IX-30	Gefahr der mangelnden Ressourcen und Know-How im Ereignisfall (Forensik, Reverse Engineering etc.)		
	GF-IX-31	Mangelndes übergeordnetes Sicherheitslagebild		

Gefahrenfeld-X: Compliance politisch-rechtliche Gefahren

Gefahrenfeld-X Compliance politisch-rechtliche Gefahren				
Subkategorie	Nr.	Gefahren	Referenz	Bemerkung
	GF-X-01	Änderungen an der Gesetzeslage national/international bzw. die notwendigen Anpassungen im Rahmen derer		
	GF-X-02	Compliance with legal and contractual requirements	ISO-27002-18.1	
	GF-X-03	Gefahr von Deifiziten bei Information security reviews	ISO-27002-18.2	
	GF-X-04	Gefahr durch Folgen eines Security Shutdowns	ENISA-GL-4.1.27	finanzielle, organisatorische bzw. auch medizinische Aspekte
	GF-X-05	Gefahr von Internetsperren im In- und Ausland		TSM-Verordnung: Ausnahme für Sicherheitsaspekte
	GF-X-06	Gefahr von rechtlichen Eingriffen in das Internet (Netzneutralität)		
	GF-X-07	Gefahr von urheberrechtlichen Einschränkungen und Vorgaben für den Telekom- und ISP-Bereich		

Gefahrenfeld-X Compliance politisch-rechtliche Gefahren				
Subkategorie	Nr.	Gefahren	Referenz	Bemerkung
	GF-X-08	Gefahr der Eingriffe von Sicherheits- und Strafverfolgungsbehörden (Abhöreinrichtungen) stellen ein zusätzliches Sicherheitsrisiko dar(Vorratsdatenspeicherung etc.)		Backdoors in Verschlüsselungsverfahren, auch Zugriff von Notrufträgern auf Standortdaten
	GF-X-09	Gefahr, dass aufgrund von nicht klar geregelten Haftungsfragen, technische Innovationen, die der Sicherheit dienen, nicht eingeführt werden		
	GF-X-10	Gefahr, dass aufgrund von (fehlender) Regulatorvorgaben (auch finanzielle Rahmenbedingungen), technische Innovationen, die der Sicherheit dienen, nicht eingeführt werden		auch bei auslaufender Technik z.B. ATM und SDH, Legacy-Systeme
	GF-X-11	Gefahr der Erpressung/Drohung/Angriffe von staatlich unterstützen Organisationen gegen die österreichische/EU IKT-Branche		
	GF-X-12	Rechtsunsicherheit inkl. Rechtsinterpretation/Rechtssprechung durch Behörden/hausinterner Juristen infolge unklarer rechtlicher Bedingungen		Use Case: Beschlagnahme von IT Infrastruktur VIP 1997, oder amerikanisches Unternehmen betreibt Rechenzentrum in EU, kann US-Behörde Herausgabe von Daten fordern?
	GF-X-13	Gefahr von hohen finanziellen Schäden durch Data Breach-Szenarien und Sicherheitsvorfälle (gem. NIS-RL)		DSG, Datenschutzgrundverordnung, Cybersicherheitsgesetz etc.

Gefahrenfeld-X Compliance politisch-rechtliche Gefahren				
Subkategorie	Nr.	Gefahren	Referenz	Bemerkung
	GF-X-14	Gefahr der erschwerten Rückverfolgung von Sicherheitsvorfällen durch extreme Datenschutzvorgaben		
	GF-X-15	Widersprüche in rechtlichen Anforderungen inkl. überstaatlicher/internationaler Problemfelder		z.B. Aktiengesetz vs. Notification-Anforderungen, SOX
	GF-X-16	Kontrahierungszwang		
	GF-X-17	Gefahr der unvorhergesehenen Verzögerung bei Behördengenehmigungen		
	GF-X-18	Ungewollte Datenweitergabe durch menschliche Fehlleistung und damit verbundene Strafzahlung		
	GF-X-19	Falsche oder missverständliche Interpretation von Sicherheits-Vorfallsmeldungen		
	GF-X-20	Gefahr der Angreifbarkeit durch die fehlende Zulässigkeit von Verkehrsprofilen		"Pausengespräch" (Netzneutralität)
	GF-X-21	Gefahren durch politischen oder wirtschaftlichem Einfluss auf informeller Ebene		
	GF-X-22	Keine Regulierung bei Inverkehrbringen von Endkundengeräten		
	GF-X-23	Gefahr der mangelnden Koordination zwischen den Branchen zu IT-Security-Themen (IOT)		

Gefahrenfeld-XI: - IOT - Weiß- und Braunware

Gefahrenfeld-XI - IOT - Weiß- und Braunware				
Subkategorie	Nr.	Gefahren	Referenz	Bemerkung
	GF-XI-01	Mangelhafte Sicherheitsimplementierungen bei Kundenendgeräten, keine oder unregelmäßige Updates durch den Hersteller		Kundenendgeräte: Keine CPEs
	GF-XI-02	Mangelnde Awareness für Sicherheit bei Endkunden und mangelnde		

Gefahrenfeld-XI - IOT - Weiß- und Braunware				
Subkategorie	Nr.	Gefahren	Referenz	Bemerkung
		Dokumentation von Endgeräten für Sicherheit		
	GF-XI-03	Mangelnder Datenschutz durch die Hersteller (Registrierungszwang bei Aktivierung)		
	GF-XI-04	Fehlende Ansprechpartner bei Gewährleistung und Produkthaftung		
	GF-XI-05	Absichtliche Backdoors durch Hersteller		
	GF-XI-06	Gefahr der globalen Erreichbarkeit von Endkundengeräten		IPV6 usw.
	GF-XI-07	Unsichere Default-Konfigurationen		
	GF-XI-08	Code Reuse bei Endkundengeräten		
	GF-XI-09	Hacking durch Endkunden		
	GF-XI-10	Cloud-basierte Devices		
	GF-XI-11	Erhöhter personeller Ressourcenaufwand durch erhöhte Anzahl von IOT-Devices		
	GF-XI-12	Missbrauch von Kundenendgeräten für Angriffe im Internet		
	GF-XI-13	Gefahr der frequency saturation durch massiv viele IOT-Geräte (Sensoren)		
	GF-XI-14	Gefahr durch unvorhergesehene Kaskaden durch neue Technologien und neuer Marktteilnehmer		Mögliche Beeinflussung der Energie-Versorgung inkl. Umwelteinflüsse auf Applikationen z.B. Parkplatz-Sensoren
	GF-XI-15	Gefahr der nicht-Nachweisbarkeit der Verschuldensfrage bei Nutzung von IOT-Geräten (DSGV)		
	GF-XI-16	Gefahr der massiven gegenseitigen Beeinflussung von Funketzen durch die Nutzung von IOT-Technologie		
	GF-XI-17	Physische Unmöglichkeit IOT-Devices zu updaten		

Gefahrenfeld-XI - IOT - Weiß- und Braunware				
Subkategorie	Nr.	Gefahren	Referenz	Bemerkung
	GF-XI-18	Unerwartete Reaktionen durch "Abnicken" von AGBs		
	GF-XI-19	Fehlfunktion von Geräten infolge Kommunikationsausfall		Könnte Haftungsfrage für ISP ergeben

Anhang 3: Risikobewertungskriterien

Eintrittswahrscheinlichkeiten & Machbarkeit

Bewertungstabelle der Eintrittswahrscheinlichkeiten und Machbarkeiten						
Technische Gefahren- und Naturgefahren				Machbarkeit Intentionale Gefahren		Bewertung Punkte
Eintritts-wahrscheinlichkeit	Verbale Beschreibung	Mind. Häufigkeit 1 mal pro		Verbale Beschreibung	Aufwand in Zeit und Know-how	
unwahrscheinlich	Das Ereignis bzw. die Gefahr ist unwahrscheinlich und tritt einmal in 10-20 Jahren auf.	10-20 Jahren oder seltener		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 / Expert*innen-niveau vgl. auch State Actors inkl. gezielter Aufklärung	**1**
selten	Das Ereignis bzw. die Gefahr ist selten und tritt einmal in 5 Jahren auf.	5 Jahren		Hoher Aufwand für die Tatausführung. Setzt Wissen voraus, das man sich durch intensive Beschäftigung mit der Materie aneignen kann. Die Tat setzt voraus, dass man 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**

Bewertungstabelle der Eintrittswahrscheinlichkeiten und Machbarkeiten						
Technische Gefahren- und Naturgefahren				Machbarkeit Intentionale Gefahren		Bewertung Punkte
Eintritts-wahrscheinlichkeit	Verbale Beschreibung	Mind. Häufigkeit 1 mal pro		Verbale Beschreibung	Aufwand in Zeit und Know-how	
gelegentlich	Das Ereignis bzw. die Gefahr ist denkbar und tritt mittelfristig einmal in 2 Jahren auf.	2 Jahren		Überschaubarer Aufwand für die Tatausführung. Das Ziel hat subjektiv eine gewisse Attraktivität. Die Tat setzt voraus, dass bekannte Schwachstellen in organisatorischen IKT Barrieren mitbekannten Hilfsmittel überwunden werden müssen. (Keine Automatisation der Angriffe/Vektoren)	Tage der Vorbereitung-Fachkenntnisse werden vorausgesetzt. Auch kriminelle Handlungen	**3**
öfters	Das Ereignis bzw. die Gefahr ist möglich und tritt einmal im Quartal auf.	Quartals-weise		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	Das Ereignis bzw. die Gefahr ist bekannt und tritt wöchentlich auf.	Wöchent-lich		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		

Bewertungen der Auswirkungen

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. Wieder-		**2**
hoch	herstellungsaufwand gering. Eingesetzte Sicherungs-Technik grundsätzlich weiterhin nutzbar	Primärschaden 0,1-2% Jahresumsatz			**3**
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. Eingesetze Sicherungs-Technik muss angepasst werden. Keine grundsätzliche Änderung von Architekturen notwendig.	Primärschaden 5-10% Jahresumsatz, Kapitalmaßnahmen durch den jur. Eigentümer erforderlich	**4**

Bewertung der Auswirkungsdimension					
Auswirkung	**Verbale Beschreibung qualitativ**			**Beschreibung quantitativ**	**Bewertung Punkte**
	Verfügbarkeit	**Vertraulichkeit**	**Integrität**		
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. Eingesetze 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) mal (Ausfall in Stunden) [%h]					
Unter Sicherungs-Technik wird ein Überbegriff verstanden der auch kryptografische Techniken einschließt					

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 Informationssicherheit in Deutschland
CERT	Computer Emergency Response Team
CPE	Costumer Premises Equipment
CSP	Cybersecurity Plattform
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
NISG	Netz- und Informationssicherheitsgesetz
NISV	Netz- und Informationssicherheitsverordnung
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
RED	Radio Equipment Directive
SKKM	Staatliche Krisen und Katastrophenmanagement
TELKO	Telekommunikationsprovider
TK-Anlagen	Telekommunikationsanlagen
USV	Umfassenden 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
- 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, SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY Information and network security – Security management
- Lit.RTR-17, SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY Telecommunication security
- 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, Telekommunikationsgesetz 2021 – TKG 2021, https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20011678
- 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, NISV-Factsheets 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, RED 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 Branchenrisikoanalyse 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

» Lit.RTR-37, RICHTLINIE (EU) 2022/2555 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie) https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022L2555&qid=1674579731975&from=EN