Entwicklung eines generischen Risk Assessment Prozesses für schutzbedürftige IT-Systeme in Kernkraftwerken und Zwischenlagern

GRS - 819

Gesellschaft für Anlagen-
und Reaktorsicherheit
(GRS) gGmbH

Entwicklung eines generischen Risk Assessment Prozesses für schutzbedürftige IT-Systeme in Kernkraftwerken und Zwischenlagern

Henriette Gatz
Laura Kleinert
Claudia Quester
Oliver Rest
Birte Ulrich

März 2026

Anmerkung:

Das diesem Bericht zugrunde liegende Eigenforschungsvorhaben wurde mit Mitteln des Bundesministeriums für Umwelt, Klimaschutz, Naturschutz und nukleare Sicherheit (BMUKN) unter dem Förderkennzeichen 4722R01550 durchgeführt.

Die Verantwortung für den Inhalt dieser Veröffentlichung liegt bei der GRS.

Der Bericht gibt die Auffassung und Meinung der GRS wieder und muss nicht mit der Meinung des BMUKN übereinstimmen.

GRS - 819
ISBN 978-3-911727-12-9

Deskriptoren

Cybersecurity, IT-Sicherheit, kerntechnische Anlagen, Risk Assessment, Risk Management

Inhaltsverzeichnis

1 Einführung

Deutsche kerntechnische Anlagen sehen sich einer Vielzahl von Risiken ausgesetzt. Für die Risiken im Zusammenhang mit Störmaßnahmen oder sonstigen Einwirkungen Dritter (SEWD) mittels IT-Angriffen stehen vor allem unerwünschte Auswirkungen in Bezug auf den Missbrauch des Gefahrenpotenzials zu kriminellen, terroristischen oder weiteren maliziösen Zwecken im Fokus. Hieraus leiten sich die in § 42 AtG / ATG22n01/ genann-ten Schutzziele der Sicherung kerntechnischer Anlagen ab, welche die Freisetzung von Kernbrennstoffen oder ihrer Folgeprodukte in erheblichen Mengen sowie die Entwen-dung von Kernbrennstoffen zum Zwecke der späteren Freisetzung oder der Herstellung einer kritischen Anordnung als zu verhindernde Auswirkungen von potenziellen Angriffen nennen. Darüber hinaus gibt es im Hinblick auf SEWD mittels IT-Angriffen noch weitere unerwünschte Auswirkungen, deren Verhinderung zwar nicht gesetzlich gefordert wird, wohl aber im Interesse der Genehmigungsinhaber liegt. Vor dem Hintergrund jeder zu verhindernden Auswirkung ist eine Betrachtung und Einschätzung des Risikos, d. h. des Potenzials für das Eintreten dieser Auswirkungen durch die Realisierung einer beste-henden Bedrohung, wesentlich. Für ein solches Risk Assessment spielen nicht nur die Bedrohungen an sich, sondern auch die Angriffsoberfläche, d. h. die Summe aller möglichen Angriffsvektoren und die implementierten Sicherungsmaßnahmen eine wichtige Rolle.

Die IT-Bedrohungslage in Bezug auf industrielle Steuerungssysteme und kritische Infra-strukturen /BSI21r02, GRS21r16, GRS23r02, GRS24r02/ und damit auch die Situation, der die deutschen kerntechnischen Anlagen und Einrichtungen in Bezug auf potenzielle IT-Sicherheitsvorfälle gegenüberstehen, entwickelt sich sehr dynamisch. In den vergan-genen Jahren wurden vermehrt gezielte IT-Angriffe auf industrielle Steuerungssysteme in kritischen Infrastrukturen beobachtet. Die IT-Bedrohungslage spiegelt dabei eine Viel-zahl von Aspekten wie beispielsweise IT-Angriffswerkzeuge, Schadsoftwarekomponen-ten, IT-Sicherheitsvorfälle, IT-Angriffe, und Aktivitäten von Advanced Persistent Threats[1] (APT) wider. Zum anderen vergrößert sich die Angriffsoberfläche, d. h. die Summe aller potenziellen Angriffsvektoren, stetig, wobei insbesondere die wachsende Digitalisierung und der Einsatz rechnerbasierter industrieller Steuerungssysteme, das Outsourcing von sensitiven Diensten, die zunehmende Nutzung von Remote-Verbindungen und

[1] Unter advanced persisten threat versteht man eine über lange Zeit andauernde Bedrohung durch Akteure mit fortgeschrittenen Fähigkeiten

softwarebedingte Alterungseffekte eine Rolle spielen. Zusätzlich zeigt sich, dass Schwachstellen in industriellen Steuerungssystemen oder anderen Komponenten und Einrichtungen auftreten, die in kerntechnischen Anlagen zum Einsatz kommen. Ebenso werden vielfach Schwachstellen in Komponenten, Programmen und Betriebssystemen bekannt, die ebenfalls innerhalb der IT-Infrastruktur solcher Anlagen eingesetzt sind. Häufig werden diese Schwachstellen bereits lange vor ihrem Bekanntwerden unbemerkt genutzt. Hinzu kommt, dass Schwachstellen in vielen Fällen sehr spät oder gar nicht gepatcht werden, sodass sie auch noch Jahre nach ihrem Bekanntwerden für Angreifer interessant sind und entsprechend ausgenutzt werden. Mit dem Auftreten solcher Schwachstellen gehen gewisse Risiken für die Betreiber kerntechnischer Anlagen einher, die entsprechend betrachtet werden müssen. Kritische Infrastrukturen sind mittlerweile häufig von IT-Angriffen betroffen, wobei unter anderem derartige Schwachstellen ausgenutzt werden. Darüber hinaus setzen Angreifer außerdem weitere Techniken ein, die unabhängig von diesen Schwachstellen sein können. Dabei rückt insbesondere die Ausspähung, Manipulation, Disruption oder Sabotage von industriellen Steuerungssystemen immer stärker in den Fokus von IT-Angreifern. Die beobachteten IT-Sicherheitsvorfälle und IT-Angriffe der vergangenen Jahre /GRS21r16, GRS23r02, GRS24r02/ zeigen deutlich, dass es mittlerweile verschiedene Angreifer-Gruppierungen gibt, die in der Lage sind, komplexe und über lange Zeiträume unentdeckte IT-Angriffe auszuführen, die – sofern dies zum Ziel der Angreifer zählt – sich auch auf industrielle Steuerungssysteme erstrecken. Unter den in den vergangenen Jahren bekannt gewordenen IT-Sicherheitsvorfällen und IT-Angriffen befindet sich eine stetig wachsende Zahl an IT-Sicherheitsvorfällen und IT-Angriffen mit Relevanz für deutsche kerntechnische Anlagen und Einrichtungen. Dies schließt neben IT-Sicherheitsvorfällen mit direktem kerntechnischem Bezug sowohl IT-Angriffe auf andere kritische Infrastrukturen als auch IT-Angriffe auf industrielle Steuerungssysteme oder deren Lieferkette mit ein.

Vor diesem Hintergrund wurden in den letzten Jahren viele internationale Standards und Richtlinien zur Informationssicherheit aktualisiert, um solchen Veränderungen in der Bedrohungslage zeitnah begegnen zu können. Ein wirkungsvolles Instrument, um auf die jeweils aktuelle IT-Bedrohungslage zu reagieren, ist die Durchführung von anlagenspezifischen Risk Assessments und Risk Managements unter Einbeziehung tatsächlich vorhandener IT-Systeme, aktueller Bedrohungen, Angriffsszenarien und Schwachstellen sowie möglicher Auswirkungen einer Kompromittierung der IT-Systeme auf die Sicherheit und Sicherung der Anlage.

Parallel zur ständig wachsenden Bedrohung durch IT-Angriffe auf kritische Infrastrukturen und auch auf kerntechnische Anlagen und Einrichtungen haben der Schutz von schutzbedürftigen IT-Systemen in Kernkraftwerken vor Störmaßnahmen und sonstigen Einwirkungen Dritter (SEWD) und die hierzu realisierten Sicherungsmaßnahmen in den vergangenen Jahren stark an Bedeutung gewonnen. Für kerntechnische Anlagen und Einrichtungen der Sicherungskategorien I und II erfolgt die Feststellung des Schutzbedarfs eines schutzbedürftigen IT-Systems gemäß der SEWD-Richtlinie IT /BMU13n03/, der entsprechenden IT-Lastannahmen /BMU13n04/ und der Erläuterungen für die Zuordnung der IT-Systeme von Kernkraftwerken zu IT-Schutzbedarfsklassen /BMU13n05/. Für Zwischenlager werden zusätzlich die entsprechenden Erläuterungen /BMU17n01/ sowie für kerntechnische Anlagen und bei Tätigkeiten der Sicherungskategorie III die SEWD-Richtlinie IT SK III /BMU20n01/ herangezogen. Die Vorgehensweise gemäß IT-Richtlinie SEWD beinhaltet über die Berücksichtigung der hier genannten Erläuterungen implizit ein generisches Risk Assessment für typische schutzbedürftige IT-Systeme in den entsprechenden kerntechnischen Anlagen: Die IT-Schutzbedarfsfeststellung für jedes schutzbedürftige IT-System der kerntechnischen Anlage oder Einrichtung erfolgt auf Basis einer Bewertung hinsichtlich der maximal möglichen Auswirkungen im Hinblick auf die Schutzziele gemäß § 42 AtG /ATG22n01/, die insgesamt aus einer Kompromittierung bzw. Manipulation des IT-Systems oder den darauf vorhandenen Informationen resultieren können. Die IT-Schutzbedarfsklassen orientieren sich an diesen zu verhindernden Auswirkungen im Hinblick auf die Schutzziele gemäß § 42 AtG /ATG22n01/. Für typischerweise in Kernkraftwerken und Zwischenlagern vorhandene IT-Systeme wurde vor dem Hintergrund der Schutzziele ein generisches, auf die genannten Auswirkungen ausgerichtetes Risk Assessment durchgeführt, dessen Ergebnisse das Kernstück der Erläuterungspapiere für Kernkraftwerke /BMU13n05/ bzw. Zwischenlager /BMU17n01/ bilden. Die in den Erläuterungspapieren vorgesehene Zuordnung eines schutzbedürftigen IT-Systems, ist bei der IT-Schutzbedarfsfeststellung zu berücksichtigen und Abweichungen sind zu begründen. Solch eine Begründung muss sich zwangsläufig auf ein Risk Assessment auf Basis der konkreten, in den Anlagen eingesetzten IT-Systeme und eine entsprechende IT-Schutzbedarfsfeststellung gemäß SEWD-Richtlinien IT /BMU13n03, BMU20n01/ stützen. Sowohl für ein erstmaliges Risk Assessment als auch für die regelmäßige Überprüfung des IT-Sicherheitskonzepts und damit der bisher getroffenen Zuordnungen der IT-Systeme zu IT-Schutzbedarfsklassen sowie der sich daraus ergebenden IT-Sicherheitsmaßnahmen, ist die Durchführung eines anlagenspezifischen Risk Assessments ein wirkungsvolles Instrument.

Hierbei ist eine systematische Vorgehensweise unter Einbeziehung der aktuellen IT-Bedrohungslage sowie möglicher Auswirkungen einer Kompromittierung der IT-Systeme auf die Sicherheit und Sicherung der Anlage wesentlich. Ein generischer Risk Assessment Prozess ist damit die Grundlage der kontinuierlichen Verbesserung der IT-Sicherheitsmaßnahmen zum Schutz von IT-Systemen in kerntechnischen Anlagen und Einrichtungen vor SEWD. In internationalen und auch nationalen Regelwerken und Richtlinien wird häufig Bezug auf Risk Assessments genommen, auch gibt es einzelne Standards, die sich vornehmlich mit dieser Thematik beschäftigen. Auf Basis des deutschen kerntechnischen Regelwerks, aber auch auf Basis international etablierter Standards, ergibt sich diesbezüglich aber noch keine einheitliche Vorgehensweise.

Dieses Vorhaben ist daher auf die Entwicklung eines generischen Risk Assessment Prozesses für IT-Systeme in kerntechnischen Anlagen und Einrichtungen zur regelmäßigen und anlassbezogenen Überprüfung und Anpassung der etablierten IT-Sicherheitsmaßnahmen ausgerichtet. Die inhaltlichen Arbeiten hierzu umfassen zum einen die Ermittlung und vergleichende Darstellung von verschiedenen Ansätzen zum Risk Assessment bzw. Risk Management aus internationalen Standards, Richtlinien und Veröffentlichungen (siehe Kapitel 3 und 4) sowie darauf aufbauend die Entwicklung einer generischen Vorgehensweise für die Durchführung von Risk Managements einschließlich Risk Assessments in kerntechnischen Anlagen und Einrichtungen (siehe Kapitel 5). Bevor die inhaltlichen Arbeiten zu den recherchierten Anforderungen und Vorgehensweisen erläutert werden, werden in Kapitel 2 wesentliche Konzepte und Begriffe im Zusammenhang mit Risk-Assessment-Prozessen vorgestellt.

2 Wesentliche Konzepte und Begriffe im Zusammenhang mit Risk Assessment-Prozessen

Risiko

Risiko beschreibt das Potenzial für negative Auswirkungen (nukleare Sicherung, nukleare Sicherheit, finanzielle Aspekte etc.) durch die Realisierung einer gegebenen Bedrohung, wobei sowohl das potenzielle Schadensausmaß bei Realisierung der Bedrohung als auch die Wahrscheinlichkeit für deren Realisierung eine Rolle spielen.

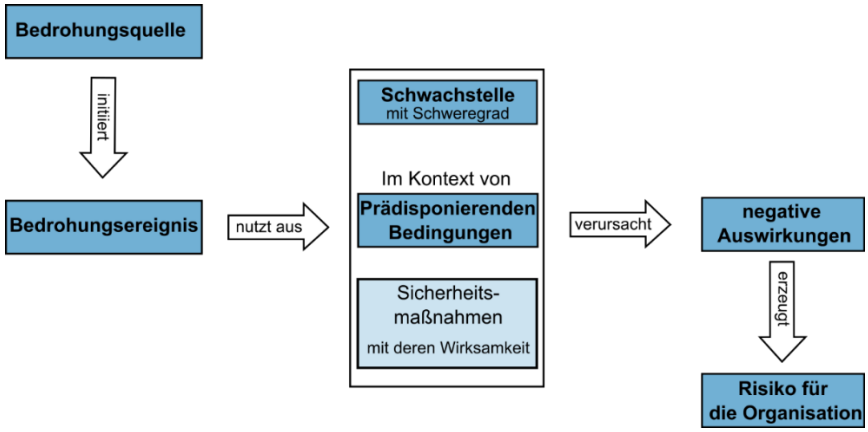

Abb. 2.1 Übersicht über den Zusammenhang zwischen Bedrohungen, Schwachstellen, Kontext, Maßnahmen, Auswirkungen und Risiken nach /NIS12n01/

Eine Bedrohung kann durch eine Bedrohungsquelle, welche ein Bedrohungsereignis initiiert beschrieben werden. Im Rahmen dieses Ereignisses wird im Kontext von prädisponierenden Bedingungen und vor dem Hintergrund der realisierten Sicherungsmaßnahmen eine oder mehrere Schwachstellen in Systemen, Prozessen oder Sicherungsmaßnahmen, die für den Angriffsvektor relevant sind, ausgenutzt. Hierdurch können potenziell negative Auswirkungen bzw. unerwünschte Konsequenzen auftreten. Das potenzielle Schadensausmaß durch die Konsequenzen und deren Eintrittswahrscheinlichkeit bestimmen das zugehörige Risiko (siehe Abb. 2.1).

Bedrohung

Der Begriff Bedrohung umfasst jeglichen Umstand oder Ereignis, durch den oder das potenziell eine unerwünschte Konsequenz eintreten kann. Bedrohungen müssen hierbei nicht zwangsläufig mit maliziösen Angreiferhandlungen oder Intentionen in

Zusammenhang stehen. Vielmehr können sie auch unabsichtliche Handlungen sowie externe Bedingungen wie beispielsweise Naturereignisse beinhalten.

IT-Angriff

Bei einem IT-Angriff handelt es sich um eine vorsätzliche Einwirkung auf eines oder mehrere IT-Systeme der Anlage oder der Beförderung, die deren Kompromittierung und/oder die Kompromittierung der von diesen IT-Systemen verarbeiteten Informationen zum Ziel hat.

IT-System

Unter IT-Systemen versteht man alle programmierbaren und/oder rechnerbasierten Komponenten oder Systeme, insbesondere auch Automatisierungs-, Prozesssteuerungs- oder Leittechniksysteme. Hierzu zählen auch alle programmierbaren und/oder rechnerbasierten Komponenten oder Systeme, die durch externe Geräte konfiguriert bzw. parametriert werden können. Ein IT-System kann ein Teilsystem eines Gesamtsystems oder einer größeren Komponente sein.

Schwachstelle

Schwachstelle bezeichnet eine Anfälligkeit oder Verwundbarkeit in einem IT-System, in sicherheits- oder sicherungsrelevanten Abläufen oder in etablierten Sicherheits- und Sicherungsmaßnahmen, die von einem Angreifer ausgenutzt werden kann. Schwachstellen sind beispielsweise insbesondere im Zusammenhang mit digitalen Systemen (Systeme zur Informationsverarbeitung, Systeme zur Automation, Leittechniksysteme etc.) relevant und ermöglichen potenziellen Angreifern durch ihre Ausnutzung verschiedene Angriffsschritte. Schwachstellen in organisatorischen Abläufen und Prozessen sowie Schwachstellen mit Bezug zum Faktor Mensch müssen ebenfalls berücksichtigt werden. Darüber hinaus stellen auch Schwachstellen in Zusammenhang mit nicht oder ungenügend umgesetzten Sicherungsmaßnahmen oder Sicherungsmaßnahmen mit verbleibenden Schwachpunkten, mögliche Angriffspunkte dar. Schwachstellen in allen Bereichen können mit der Zeit entstehen, beispielsweise durch Veränderungen im organisatorischen oder betrieblichen Umfeld, durch Änderungen im Bereich von IT-Systemen und eingesetzten Technologien sowie durch die Entwicklung oder Ausweitung von Bedrohungen.

Konsequenz

Auswirkung oder logische Folge (Veränderung oder Nicht-Veränderung) eines Ereignisses, eines Vorfalls, einer Handlung oder einer Entscheidung, die in der Regel nicht nur durch das Ereignis, den Vorfall, die Handlung oder die Entscheidung an sich, sondern auch durch die beteiligten Systeme, Menschen und Randbedingungen ermöglicht, erleichtert, verursacht, verhindert, gefördert oder verändert werden kann. Eine Konsequenz kann positiv oder negativ sein.

Wahrscheinlichkeit, Likelihood

Abgeschätzte Wahrscheinlichkeit für die Realisierung einer Bedrohung. Dabei kann sich der Begriff Wahrscheinlichkeit auf verschiedene Aspekte beziehen. Beispielsweise kann sich eine Wahrscheinlichkeit im Kontext des Risk Assessment auf die Eintrittswahrscheinlichkeit für ein Ereignis oder Szenario oder auch auf die Eintrittswahrscheinlichkeit für eine unerwünschte Konsequenz beziehen. Sie wird auch verwendet, um anzugeben, mit welcher Wahrscheinlichkeit ein Angreifer in der Lage ist, eine bestehende Schwachstelle auszunutzen oder eine bestimmte Auswirkung hervorzurufen. Vielfach wird auch die Eintrittswahrscheinlichkeit für ein Ereignis in Kombination mit der Eintrittswahrscheinlichkeit der unerwünschten Konsequenzen bei Eintritt des Ereignisses kombiniert, um die gesamte Eintrittswahrscheinlichkeit für eine unerwünschte Konsequenz anzugeben.

Sie kann qualitativ oder quantitativ angegeben werden. Bei der Verwendung des Begriffs Wahrscheinlichkeit im Kontext des Risk Assessments ist eine klare Abgrenzung im Hinblick auf die verwendete Bedeutung essenziell, insbesondere weil unterschiedliche Definitionen eine Vergleichbarkeit erschweren. Auch ist zu beachten, dass sich manche der Wahrscheinlichkeiten wie beispielsweise Eintrittswahrscheinlichkeiten für eine unerwünschte Konsequenz durch Sicherungsmaßnahmen beeinflussen lassen, während dies für andere Wahrscheinlichkeiten, wie beispielsweise Eintrittswahrscheinlichkeiten für ein Ereignis, nicht der Fall ist.

3 Recherche von Anforderungen und Vorgehensweise zur Durchführung eines Risk Assessments bzw. Risk Managements

Die Anwendung von Risk Assessment Prozessen wird sowohl international als auch länderspezifisch in einer Vielzahl von Regelwerken zur IT-Sicherheit thematisiert. Im Rahmen des Vorhabens wurde zunächst eine Auswahl von relevanten nationalen und internationalen Regelwerken getroffen, die das Thema Risk Assessment behandeln. Dabei wurden sowohl für die Kerntechnik spezifische Regelwerke als auch allgemeine Regelwerke zur IT-Sicherheit betrachtet.

Von Seiten der IAEA wurden die Standards

- NSS 17-T „Computer Security Techniques for Nuclear Facilities /IAE21n02/, NSS 42-G “Computer Security for Nuclear Security” /IAE21n01/ und
- NSS 33-T “Computer Security of Instrumentation and Control Systems at Nuclear Facilities“ /IAE18n02/

herangezogen.

In Bezug auf Veröffentlichungen von IEC und ISO sind sowohl kerntechnikspezifische als auch übergreifende Normen relevant. Im Rahmen des Vorhabens betrachtet wurden:

- IEC 62645 „Kernkraftwerke – Leittechnische und elektrische Systeme – Anforderungen an die Cybersicherheit“ /DIN20n01/,
- IEC 61511 „Funktionale Sicherheit – PLT-Sicherheitseinrichtungen für die Prozessindustrie“ /DIN19n01/,
- IEC 62443 „Industrielle Kommunikationsnetze – IT-Sicherheit für Netze und Systeme“ /IEC09n03/,
- IEC 31000 „Risikomanagement - Leitlinien“ /ISO18n04/,
- IEC 31010 „Risikomanagement – Verfahren zur Risikobeurteilung“ /IEC19n04/,
- ISO 27001 „Informationstechnik–Sicherheitsverfahren–Informationssicherheitsmanagementsysteme–Anforderungen“ /ISO17n02/,
- ISO 27002 „Informationstechnik–Sicherheitsverfahren–Leitfaden für Informationssicherheitsmaßnahmen“ /ISO17n03/, und
- ISO 27005 „Informationstechnik - IT-Sicherheitsverfahren - Informationssicherheits-Risikomanagement“ /ISO18n03/.

Neben den internationalen Standards von IAEA, IEC und ISO wurden auch deutsche Regelwerke zum Risk Assessment betrachtet. Für die Betrachtung im Rahmen dieses Vorhabens wurde ein Standard des Bundesamtes für Sicherheit in der Informationstechnik (BSI) ausgewählt:

- BSI-Standard 200-3 „Risikoanalyse auf der Basis von IT-Grundschutz“ /BSI17n02/.

Die Anwendung von Risk Assessment Prozessen wird auch im Bereich der Automobilindustrie thematisiert, daher wurden die zwei folgenden Dokumente herangezogen:

- ISO/SAE 21434 “Road vehicles – Cybersecurity engineering” /ISO21n01/ und
- ISO/IEC 18045 „Information security, cybersecurity and privacy protection – Evaluation criteria for IT security – Methodology for IT security evaluation” /ISO22n01/.

Aus diesen ausgewählten Dokumenten wurden Anforderungen an das Risk Assessment sowie Ansätze und Vorgehensweisen zur Durchführung von Risk Assessment Prozessen herausgearbeitet und zusammengestellt (siehe Abschnitt 2.2). Risk Assessments sind in den USA seit Jahren Teil der „National Strategy for Cyberspace Operations“ des US-amerikanischen Departments of Defense. Daher wurde neben den deutschen und internationalen Standards auch eine länderspezifische Vorgehensweise in die Betrachtung von Risk Assessment Vorgehensweisen mit einbezogen. Ausgewählt wurde ein US-amerikanischer Standard des National Institute of Standards and Technology (NIST), der weltweit Beachtung findet:

- NIST 800-30 „Information Security - Guide for Conducting Risk Assessments“ /NIS12n01/ zu nennen, der sich ausschließlich mit Risk Assessment Prozessen beschäftigt.

Zusätzlich wurde ein weiterer US-amerikanischer Standard des National Institute of Standards and Technology (NIST) betrachtet, welcher insbesondere Sicherungsmaßnahmen behandelt:

- NIST 800-53 „Security and Privacy Controls for Information Systems and Organizations“ /NIS20r01/

Als Basis für die vergleichende Betrachtung der unterschiedlichen Ansätze, Herangehensweisen und Blickrichtungen (siehe Kapitel 3) und als Vorbereitung für die Beschreibungen der einzelnen konkreten Vorgehensweisen, wurden zunächst für Risk Assessment Prozesse wesentliche Konzepte und Begriffe zusammengestellt und definiert (siehe Abschnitt 2.1)

3.1 Zusammenfassung ausgewählter Vorgehensweisen

Die zur Beschreibung eines Risk Assessment Prozesses verwendeten Begrifflichkeiten unterscheiden sich teilweise in den betrachteten Normen. In den folgenden Abschnitten werden zur besseren Vergleichbarkeit für gleiche Thematiken und Prozesse generell einheitliche Begriffe verwendet, wobei falls erforderlich auch Originalzitate deutscher bzw. englischer Begrifflichkeiten verwendet werden.

3.1.1 IAEA-Veröffentlichungen

Die IAEA greift verschiedene Aspekte im Zusammenhang mit Risk Assessment in Bezug auf die Cybersicherheit im nuklearen Kontext in mehreren technischen Leitfäden bzw. Leitfäden zur Umsetzung auf, wobei die Veröffentlichungen mit relevanten Bezügen zum Vorhaben in diesem Kapitel vorgestellt werden. Das Thema wird zunächst in der IAEA Nuclear Security Series No. 17-T „Computer Security Techniques for Nuclear Facilities" /IAE21n02/ im Rahmen allgemeiner Grundsätze im Zusammenhang mit der Cybersicherheit kerntechnischer Anlagen aufgegriffen und in der IAEA Nuclear Security Series No. 42-G „Computer Security for Nuclear Security" /IAE21n01/ in Bezug auf die Entwicklung und Umsetzung einer Cybersicherheitsstrategie insbesondere in Bezug zur Sicherung kerntechnischer Anlagen ausgeweitet. Zudem finden sich konkrete Bezüge zu leittechnischen Systemen und industriellen Steuerungen in der IAEA Nuclear Security Series No. 33-T „Computer Security of Instrumentation and Control Systems at Nuclear Facilities" /IAE18n02/. Im Folgenden werden die für das Vorhaben relevanten Inhalte dieser Veröffentlichungen kurz vorgestellt.

3.1.1.1 NSS 17-T „Computer Security Techniques for Nuclear Facilities,

Ein wesentliches Ziel des NSS 17-T „Computer Security Techniques for Nuclear Facilities /IAE21n02/ ist die Herausstellung der Relevanz der Cybersicherheit als fundamentaler Teil des Sicherheits- und Sicherungskonzepts für nukleare Anlagen und Einrichtungen. In diesem Zusammenhang kommt dem Risk Assessment als Teil des Risk Managements eine wesentliche Bedeutung zu. Dabei wird zunächst das Thema Cybersicherheit der Anlage als Ganzes im Rahmen des Risk Managements diskutiert, bevor die System-Ebene adressiert wird und Risk Management Strategien für beide Aspekte in Bezug auf die einzelnen Phasen des Lebenszyklus einer Anlage diskutiert werden.

Der in NSS 17-T beschriebene Prozess des Risk Assessments identifiziert und dokumentiert dabei zunächst entsprechende Bedrohungen, Schwachstellen und Auswirkungen und adressiert angemessene Sicherungsmaßnahmen im Rahmen eines schutzbedarfsabhängigen, abgestuften Ansatzes. Das Risk Assessment in Bezug auf Bedrohungen und Schwachstellen stellt die Basis für die Vorbereitung von notwendigen Sicherungsmaßnahmen zum Schutz vor oder zur Abschwächung der Auswirkungen von Angriffen auf die IT-Systeme dar. Die grundlegenden Schritte des Risk Managements für die Anlage bzw. einzelne Systeme sind gemäß NSS 17-T:

- Definition des Umfangs und Kontexts,
- Charakterisierung Anlage, Systeme und Bedrohungen
- Identifizierung von Digital Assets
- Spezifikation von Anforderungen und Maßnahmen
- Verifizierung und Validierung
- Abstimmung mit Behörden

Zur Implementierung eines systematischen und einheitlichen Risk Assessments muss ein klar definierter Prozess angewendet werden, der die existierenden Standards erfüllt. Die Notwendigkeit zur Bewertung der Systeme, die Detailtiefe des Risk Assessments und die Häufigkeit der Aktualisierung ist abhängig von der Bedeutung des Systems, insbesondere in Bezug auf die sicherheitstechnische Funktion und den Schutz der Systeme. Zudem müssen neue Analysen bei entsprechend neuen Umständen und eine Überprüfung von Änderungen/Anpassungen von Systemen im Rahmen des Risk Assessment durchgeführt werden. Zusätzliche potenzielle Bedrohungen, beispielsweise im Zusammenhang mit Schwachstellen von IT-Systemen, ergeben sich typischerweise zudem mit der Weiterentwicklung von isolierten hin zu vernetzten Systemen, was entsprechend berücksichtigt werden muss.

Im Rahmen eines Programms zur Sicherstellung der Cybersicherheit sollte gemäß NSS 17-T aufgrund der steigenden Komplexität von Angriffen und der steigenden Anzahl potenzieller Angriffsmöglichkeiten ein Risk Assessment angestrebt werden, welches eine möglichst große Bandbreite von potenziellen Angriffsszenarien abdeckt. Die ersten Schritte eines solchen Programms sollten sich darauf fokussieren, die potenziellen Bedrohungen zu verstehen. Als Basis hierfür dienen glaubwürdige Profile der Angreifer und Angriffsszenarien. Beispielsweise kann als erster Schritt eine Matrix des

Angreiferprofils erstellt werden, in der die Angreifer, deren Motivationen und potenzielle Zielobjekte aufgelistet sind. Darauf aufbauend können plausible Angriffsszenarien entwickelt werden. Zu den Faktoren, die einerseits erheblichen direkten oder indirekten Einfluss *auf* und andererseits Folgen *für* die Funktionalität und Sicherheit der IT-Systeme haben, und die die Sicherheit und den Schutz der gesamten Anlage beeinträchtigen und bei der Auswahl von Sicherungsmaßnahmen berücksichtigt werden müssen, zählen insbesondere:

- Lastannahmen (Design Basis Threat (DBT)): Die Lastannahmen beinhalten Eigenschaften und Charakteristika von potenziellen Angreifern/Bedrohungsakteuren (intern, extern). Sie sind wichtig für die Ermittlung des Ausmaßes einer Bedrohung und bilden die Basis für die Auswahl und Bemessung von Sicherungsmaßnahmen, um einen angemessenen Status in Bezug auf die Cybersicherheit zu erhalten. Sie repräsentieren u. a. die größtmögliche Bedrohung, die eine Anlage berücksichtigen und gegen die sie sich basierend auf der aktuellen Bedrohungslage schützen muss.
- Angreiferprofile: Die Angreiferprofile werden beispielweise durch Tabellen veranschaulicht. Hierbei werden sowohl Bedrohungen durch Innentäter als auch andere Arten von Angreifern berücksichtigt. Dabei werden beispielsweise die zur Verfügung stehenden Tatmittel, die Zeitspanne eines Angriffs, die Werkzeuge die wahrscheinlich verwendet werden und die Motivation des Angreifers betrachtet.
- Angriffsszenarien: Bei den Angriffsszenarien müssen mehrere potenzielle Ziele für einen Angriff auf eine kerntechnische Anlage berücksichtigt werden:
    - Vorbereitung eines später koordinierten Angriffs zur Sabotage der Anlage und/oder zur Entwendung von radioaktivem Material,
    - Gefährdung der Sicherheit von Menschen und Natur,
    - Vorbereitung eines Angriffs auf eine andere Anlage,
    - Verbreitung von Angst und Verwirrung,
    - Erreichen eines finanziellen Gewinns;

Abhängig von den Zielen des Angriffs nutzen Angreifer potenzielle Schwachstellen der unterschiedlichen eingesetzten Systemen aus, um unter anderem folgende Handlungen durchzuführen:

- illegitimer Zugriff auf Informationen (Verlust der Vertraulichkeit),
- Abfangen oder Ändern von Informationen (Verlust der Integrität),

- Verhindern der Datenübertragung und/oder das Abschalten von Systemen (Verlust der Verfügbarkeit),
- illegitimes Eindringen in das Netzwerk oder illegitimer Zugriff auf das IT-Systems;

Das grundlegende Ergebnis eines Risk Assessments ist damit eine Auflistung der Systeme, die in nuklearen Anlagen vorhanden sind, sowie der potenziellen Auswirkungen von erfolgreichen Angriffen auf diese betrachteten Systeme und die dazugehörigen Auswirkungen auf die Anlage. Dazu werden angemessene Sicherungsmaßnahmen identifiziert, um den betrachteten Bedrohungen zu begegnen. Die Erfolgswahrscheinlichkeit solcher Angriffe, sowie deren potenzielle Auswirkungen sind vom Kontext und der Anlage abhängig. Gemäß NSS 17-T sollte ein gründliches Risk Assessment insbesondere in Bezug auf die Vertraulichkeits-, Integritäts- und Verfügbarkeitsanforderungen für jedes IT-System der kerntechnischen Anlage durchgeführt werden. Es werden somit grundlegend elementare Aspekte zur Durchführung eines Risk Assessment im Kontext der Cybersicherheit einer kerntechnischen Anlage adressiert und die einzelnen Schritte und Teilaspekte wie beispielsweise im Zusammenhang mit potenziellen Bedrohungen bzw. der Charakterisierung der eigenen Anlage in Bezug auf die eingesetzten Systeme tiefergehend diskutiert.

3.1.1.2 NSS 42-G „Computer Security for Nuclear Security”

Der Leitfaden NSS 42-G der IAEA /IAE21n01/ adressiert erstmals die Cybersicherheit als Teil der Sicherung kerntechnischer Anlagen im Detail und stellt dabei unter anderem die Implementierung entsprechender Sicherungsmaßnahmen in den Fokus. Im Vergleich zu NSS 17-T /IAE21n02/ liegt der Fokus hier somit im Wesentlichen nicht bei übergeordneten Fragen zum sicheren Betrieb und der Sicherheit kerntechnischer Anlagen, sondern insbesondere beim Aspekt der Cybersicherheit als Teil der Sicherung solcher Anlagen. Für das Vorhaben relevante Inhalte finden sich dabei unter anderem in den Kapiteln zur Etablierung und Implementierung einer Cybersicherheitsstrategie sowie zur Entwicklung eines Cybersicherheitsprogramms. Im Folgenden werden die Aspekte, die einen direkten oder indirekten Bezug zum Risk Assessment haben bzw. Ähnlichkeiten in der Vorgehensweise aufweisen und ein Teil der o. g. in NSS 42-G diskutierten Cybersicherheitsstrategie sind, kurz zusammengefasst.

In Bezug auf die Etablierung einer Cybersicherheitsstrategie werden in NSS 42-G verschiedene Punkte adressiert, die entsprechend zu berücksichtigen und bei der

Entwicklung aufzugreifen sind. Dazu zählen unter anderem Informationen zur Art der Durchführung eines Assessments möglicher Bedrohungen, einschließlich der Identifizierung potenzieller Cyber-Angriffsszenarien, Vorgehensweisen zur Bestimmung relevanter Zielsetzungen in Bezug auf die Cybersicherheit und Maßnahmen zur Aufrechterhaltung der entsprechenden Fähigkeiten in Bezug auf die Cybersicherheit innerhalb des Kontextes der nuklearen Sicherung. Dazu werden vorbereitende Schritte genannt, die relevant für die Etablierung der Cybersicherheitsstrategie sind. Diese umfassen unter anderem die konkrete Durchführung eines Assessments der Bedrohungen und die Bewertung der Auswirkungen eines Angriffs auf schutzbedürftige IT-Systeme auf die Sicherung kerntechnischer Anlagen.

In Bezug auf das Assessment potenzieller Bedrohungen der Cybersicherheit werden in NSS 42-G mehrere Empfehlungen gegeben, die sich im Wesentlichen an staatliche Einrichtungen richten und eine Grundlage für weitergehende Betrachtungen der Betreiber bilden. Demnach soll der Staat unter anderem ein stets aktualisiertes Assessment der Bedrohungen für den Bereich der nuklearen Sicherheit aufrechterhalten und diese Informationen in die Entwicklung von Lastannahmen einfließen lassen. Die vom Staat erstellten Bedrohungsanalysen und/oder Lastannahmen sollen dabei neben externen Angreifern auch die Möglichkeit von Angriffen durch Innentäter oder kombinierte Angriffe beinhalten. Das Assessment soll regelmäßig vom Staat aktualisiert werden, wobei die Häufigkeit der Überprüfung abhängig vom Fortschritt der Technik, neuentdeckten Schwachstellen und Änderungen der Bedrohungslage ist. Insgesamt soll der Staat nach Empfehlungen in NSS 42-G sicherstellen, dass das Assessment potenzieller Bedrohungen und/oder die Lastannahmen in Bezug auf die Cybersicherheit genügend Details für das nachfolgende Risk Assessment liefert, um zu einem angemessenen und wirksamen Maß bzgl. der Cybersicherheit zu gelangen. Letztendlich wird in NSS 42-G bei der Diskussion des Assessments potenzieller Bedrohungen, die Verantwortung für den Schutz gegen diese, klar zwischen von Betreibern zu leistenden Schutzmaßnahmen und vom Staat zu übernehmenden Aufgaben, getrennt.

Im Rahmen des Vorhabens ist außerdem insbesondere der Abschnitt zur Risk Assessment Methodik zur Bestimmung von Sicherungsmaßnahmen relevant. Dabei gilt es zunächst die entsprechende Methodik festzulegen, anhand derer die betroffenen Anlagen die ersten Schritte im Rahmen des Risk Management durchführen. Dazu zählen die Ermittlung, ob ein rechnerbasiertes System sicherheitstechnisch relevante Funktionen besitzt, die Feststellung, ob jedes der identifizierten Systeme schutzbedürftig ist, und die

Durchführung einer Risikoanalyse zur Ermittlung des Ausmaßes der notwendigen Sicherungsmaßnahmen für schutzbedürftige IT-Systeme. Die Methodik sollte gemäß NSS 42-G zudem Folgendes berücksichtigen:

- Einschlägige Gesetze und Richtlinien,
- die Wichtigkeit der Funktionen der schutzbedürftigen IT-Systeme, einschließlich der Bedeutung des Schutzes der Vertraulichkeit, Integrität und Verfügbarkeit,
- eine Bewertung der Auswirkungen von Angriffen auf schutzbedürftige IT-Systeme,
- die Betriebsumgebung der schutzbedürftigen IT-Systeme,
- Identifizierung und Bewertung der relevanten Bedrohungen,
- die Attraktivität der schutzbedürftigen IT-Systeme für Bedrohungsakteure in Bezug auf die nukleare Sicherung,
- Schwachstellen der schutzbedürftigen IT-Systeme;

Dabei sollten unterschiedliche Möglichkeiten der Kompromittierung schutzbedürftiger IT-Systeme berücksichtigt werden, welche in weiterer Folge das Ergebnis des Risk Assessments beeinflussen können:

- die Funktionen der schutzbedürftigen IT-Systeme sind undefiniert,
- schutzbedürftige IT-Systeme zeigen unerwartete Verhaltensweisen oder Aktionen,
- Ausfall der schutzbedürftigen IT-Systeme,
- schutzbedürftige IT-Systeme sind fehlertolerant und verhalten sich wie ursprünglich beabsichtigt;

Das Risk Assessment sollte gemäß NSS 42-G alle relevanten Aspekte der Sicherung umfangreich berücksichtigen, wie beispielsweise potenzielle Innentäter sowie kombinierte Angriffe, bei denen Angreifer sowohl konventionelle wie auch Cyberangriffshandlungen ausführen.

Weiterhin werden in NSS 42-G Aspekte in Bezug auf das Risk Assessment durch Organisationen adressiert. Das generelle Ziel des Risk Assessments für Organisationen umfasst demnach unter anderem die folgenden Punkte:

- Identifizierung und Verständnis der Risiken, sowie der Faktoren, die zu diesen Risiken beitragen,

- Erlangung einer Basis zur Identifizierung von (schutzbedürftigen) IT-Systemen,
- Definition einer Grundlage auf Basis derer Veränderungen von (schutzbedürftigen) IT-Systemen überwacht und analysiert werden können inklusive Betrachtungen zu resultierenden Auswirkungen auf die nukleare Sicherung.

Das Risk Assessment kann dabei sowohl auf organisatorischer Ebene als auch auf der Systemebene durchgeführt werden, wobei es sich auf die nationale Bedrohungslage und/oder die Lastannahmen stützen und andere verfügbare Informationsquellen über Cyber-Bedrohungen berücksichtigen sollte. Beim Risk Assessment sollten die nachteiligen Folgen für die nukleare Sicherheit oder die nukleare Sicherung berücksichtigt werden, die sich aus der Kompromittierung und/oder dem Fehlbetrieb jedes IT-Systems ergeben, was bei der Identifizierung von schutzbedürftigen IT-Systemen entsprechend zu berücksichtigen ist. Auch beim Risk Assessment durch die Organisationen sollten alle Aspekte der nuklearen Sicherung, einschließlich z. B. des physischen Schutzes und Innentäter-Szenarien zusammen mit der Cybersicherheit gemeinsam betrachtet werden, um das Risiko von kombinierten Angriffen zu bewerten.

Insgesamt werden somit in NSS 42-G wichtige Aspekte zur Durchführung eines Risk Assessment im Kontext der Cybersicherheit einer kerntechnischen Anlage adressiert und die einzelnen Schritte und Teilaspekte wie beispielsweise die Identifizierung schutzbedürftiger IT-Systeme oder die Betrachtung von Bedrohungen als Ausgangspunkt für das weitere Vorgehen werden diskutiert. Zudem befasst sich das Dokument neben Empfehlungen für Organisationen für das entsprechende Vorgehen auch mit Empfehlungen für Behörden.

3.1.1.3 NSS 33-T „Computer Security of Instrumentation and Control Systems at Nuclear Facilities”

Der NSS 33-T “Computer Security of Instrumentation and Control Systems at Nuclear Facilities” /IAE18n02/ behandelt das Thema Cybersicherheit für leittechnische Systeme, die im Zusammenhang mit der Sicherheit und Sicherung in kerntechnischen Anlagen eingesetzt werden. Im Vergleich zu den oben genannten IAEA-Veröffentlichungen NSS 17-T /IAE21n02/ und NSS 42-G /IAE21n01/, die allgemein auf unterschiedliche IT-Systeme in kerntechnischen Anlagen ausgerichtet sind, legt NSS 33-T den Fokus auf industrielle Steuerungssysteme und leittechnische Einrichtungen, die im Wesentlichen Überwachungs- und/oder Steuerungsfunktionen für den Betrieb der Anlage ausüben.

Da durch diese Systeme je nach den genauen Umständen durch potenzielle Angreifer auch physikalische Prozesse beeinträchtigt werden können, sind diese Systeme in der Regel schutzbedürftig und müssen entsprechend auch vor Bedrohungen im Rahmen möglicher Cyberangriffe geschützt werden. Im Folgenden werden die Aspekte, die einen direkten oder indirekten Bezug zum Risk Assessment haben bzw. Ähnlichkeiten in der Vorgehensweise aufweisen und somit relevant für das Vorhaben sind, kurz zusammengefasst.

In NSS 42-G werden unter anderem Schlüsselkonzepte in Bezug auf die Cybersicherheit von leittechnischen Systemen beschrieben, wobei hinsichtlich der Auslegung von Sicherungsmaßnahmen unter Berücksichtigung eines Graded Approach verschiedene Anforderungen auf Basis einer risikobewussten Herangehensweise genannt werden. Diese Anforderungen umfassen unter anderem Aspekte, die unter anderem im Rahmen eines Risk Assessments relevant sind und Ergebnis desselben sein können:

- Betrachtung der Wichtigkeit der leittechnischen Funktionen für die Sicherheit und Sicherung der kerntechnischen Anlage,
- Betrachtung der identifizierten und bewerteten Bedrohungen für die Anlage,
- Betrachtung der Attraktivität der leittechnischen Systeme für potenzielle Angreifer,
- Betrachtung der Schwachstellen der leittechnischen Systeme,
- Betrachtung der potenziellen Auswirkungen, die direkt oder indirekt aus einer Kompromittierung eines Systems resultieren können;

Das Thema Risk Assessment wird außerdem im Kapitel zum „Risk Informed Approach“ in Bezug auf die Cybersicherheit von leittechnischen Systemen aufgegriffen. Demnach kann ein risikobasierter Ansatz für die Cybersicherheit von leittechnischen Systemen Vorgehensweisen eines Risk Assessments zur Identifizierung von Schwachstellen einer Anlage, die mit Cyberattacken auf diese Systeme in Zusammenhang stehen, ausnutzen und die Auswirkungen, die aus der erfolgreichen Ausnutzung der Schwachstellen resultieren können, bestimmen. Maßnahmen in Bezug auf die Cybersicherheit können entsprechend anhand der Ergebnisse eines Risk Assessments zugewiesen werden.

In NSS 33-T werden im Abschnitt zu „Computer security assessments“ außerdem Empfehlungen für Vorgehensweisen ausgesprochen, die direkten Bezug zum Risk Management bezogen auf die Cybersicherheit haben und entsprechend auch Ähnlichkeiten zu einzelnen Aspekten eines Risk Assessments aufweisen.

Diese sollen für alle leittechnischen Systeme, Komponenten und Subsysteme, die als schutzbedürftig identifiziert wurden, berücksichtigt werden. Folgende Empfehlungen werden gegeben:

- Das Assessment sollte für jede Phase des Lebenszyklus durchgeführt werden, um potenzielle Bedrohungen, Schwachstellen und Mängel zu identifizieren.
- Öffentliche oder Open Source Informationen, sowie Hersteller-, Auftragnehmer-, Lieferanten- und Expertenquellen sollten überwacht werden, um sofort Änderungen der Bedrohungslage oder neue Schwachstellen zu identifizieren.
- Neue oder veränderte Bedrohungen und Schwachstellen sollten zur Evaluierung ihrer potenziellen Auswirkungen auf die Cybersicherheit von leittechnischen Systemen bewertet werden. Korrigierende Maßnahmen sollten durchgeführt werden, wenn diese Änderungen in potenziellen Verletzungen der Sicherheit resultieren oder nicht-akzeptierbare Risiken für die Anlage darstellen.
- Jede Organisation, die für die Entwicklung, den Einsatz, die Bedienung, die Instandhaltung und/oder die Stilllegung von leittechnischen Systemen oder Komponenten verantwortlich ist, sollte periodische Audits und Assessments der Informationssicherheit durchführen.
- Die Ergebnisse des Assessments sollten verwendet werden, um das Cybersicherheits-Risk Management entsprechend zu aktualisieren.

Insgesamt ergeben sich in NSS 33-T somit wichtige Aspekte und Empfehlungen zu Vorgehensweisen, die im Rahmen des Risk Managements für die Durchführung eines Risk Assessment im Kontext der Cybersicherheit einer kerntechnischen Anlage relevant sind. Diese einzelnen Aspekte werden im Kontext von NSS 33-T im Wesentlichen hinsichtlich der allgemeinen Cybersicherheit von leittechnischen Systemen in kerntechnischen Anlagen betrachtet und berühren dabei Bereiche, die für ein Risk Assessment relevant sind. Es wird jedoch keine direkte strukturierte Vorgehensweise bzw. Abfolgen entsprechender Schritte zur Durchführung in diesem Zusammenhang beschrieben.

3.1.2 IEC 62645 „Kernkraftwerke – Leittechnische und elektrische Systeme – Anforderungen an die Cybersicherheit“

Die Norm IEC 62645 „Kernkraftwerke – Leittechnische und elektrische Systeme – Anforderungen an die Cybersicherheit“ /DIN20n01/ enthält Anforderungen und Leitlinien für die Entwicklung und das Management effektiver IT-Sicherheitsprogramme für

programmierbare digitale leittechnische Systeme. In dieser Norm werden unter anderem angemessene Maßnahmen zur Verhinderung und Erkennung von und Reaktion auf Cyberangriffe festgelegt. Dies beinhaltet sowohl unsichere Situationen, Beschädigungen von Geräten oder Beeinträchtigungen der Leistungsfähigkeit der Anlage, die sich aus Angriffshandlungen ergeben können, als auch Bedienfehler, welche die Cybersicherheit verletzen und/oder Cyberangriffe erleichtern können. Generell wird das Thema Risk Assessment an mehreren Stellen in /DIN20n01/ aufgegriffen.

Zunächst soll gemäß /DIN20n01/ ein Programm für die Sicherheit programmierbarer leittechnischer Systeme im kerntechnischen Kontext auf der Grundlage eines Risk Assessments entwickelt werden. Dabei wird eine abgestufte Vorgehensweise (graded approach) für schutzbedürftige Systeme empfohlen. Das Risk Assessment und damit einhergehende Bewertungen hinsichtlich potenzieller Bedrohungen und Schwachstellen soll gemäß /DIN20n01/ bei den Überlegungen zum graded approach berücksichtigt werden, wodurch sich entsprechende Anforderungen an die Sicherung und Sicherungsmaßnahmen ergeben. Das Programm für die Sicherheit programmierbarer leittechnischer Systeme im kerntechnischen Kontext umfasst weiterhin eine Vielzahl unterschiedlicher Aspekte. Hierzu gehören beispielsweise die Entwicklung und Durchführung eines Prozesses für das Risk Assessment der sowohl die Gesamtheit der leittechnischen Systeme, sowie individuell für jedes einzelne leittechnische System, die Lastannahmen (DBT) (wo anwendbar) berücksichtigt. Das Risk Assessment in Bezug auf die Cybersicherheit sollte gemäß /DIN20n01/ von einem „Computer System Security Officer“ (CSSO) durchgeführt werden.

In Bezug auf den Schutzbedarf eines programmierbaren digitalen leittechnischen Systems, muss gemäß /DIN20n01/ dieser im Rahmen des Programms für die Sicherheit programmierbarer leittechnischer Systeme im kerntechnischen Kontext basierend auf den maximalen Folgen eines erfolgreichen Cyberangriffs auf das System in Bezug auf die Anlagensicherheit und -leistungsfähigkeit zugeordnet werden. Abgestufte Anforderungen an die Cybersicherheit werden für die unterschiedlichen Schutzbedarfsklassen festgelegt. Zudem muss im Rahmen des Risk Assessments eine Schwachstellenbewertung (Vulnerabilty Assessment) und eine Identifizierung von potenziellen Bedrohungen durchgeführt werden. Risk Assessments können dabei eine notwendige Änderung der geplanten oder etablierten Cybersicherheitsanforderungen und -maßnahmen zur Folge haben.

In /DIN20n01/ werden zudem Anforderungen an das anlagenspezifische Risk Assessment definiert, welche mindestens die folgenden Schritte abdecken sollen:

- Bestimmung von Umfang und Kontext,
- Identifizierung und Charakterisierung der Bedrohungen,
- Bewertung der Schwachstellen,
- Ausarbeitung von Angriffsszenarien,
- Abschätzung des Risikoniveaus,
- Definition der Gegenmaßnahmen;

Dabei sollen die spezifischen Verfahren und Werkzeuge des Risk Assessments festgelegt und auf dem neusten Stand gehalten werden. Über den gesamten Lebenszyklus der leittechnischen Systeme sollen wiederkehrend Neubewertungen des Risikos durchgeführt werden, wenn Systemänderungen vorgenommen oder Änderungen an der Bedrohungslage erkannt werden. Zu diesen Änderungen gehören beispielsweise neue Bedrohungen oder Schwachstellen, die die installierten, programmierbaren digitalen leittechnischen Systeme beeinträchtigen können. Das Risk Assessment, die Risikobehandlung und der graded approach sollen gemäß /DIN20n01/ nach der oben genannten Planung umgesetzt und aufrechterhalten werden.

Abschließend werden in /DIN20n01/ in Bezug zu verschiedenen Phasen des Lebenszyklus von leittechnischen Systemen mehrere Bezüge zum Thema Risk Assessment hergestellt. Beginnend bei der Design-Phase sollen demnach sämtliche Überlegungen hinsichtlich der Angemessenheit zu den Sicherheitsanforderungen das Risk Assessment berücksichtigen, welches entsprechend Schwachstellenanalysen der technischen Implementierung und spezifische Analysen zu Bedrohungs- und Angriffsszenarien (einschließlich der länderspezifischen Lastannahmen/DBT) einschließt. Risk Assessments können zudem in dieser Phase dazu führen, dass die Sicherungsmaßnahmen oder die gesamte Architektur angepasst werden müssen. Dementsprechend sollen im Rahmen von Bedrohungs- und Schwachstellen Assessments als Teil des Risk Assessments ggf. erforderliche zusätzliche Sicherungsmaßnahmen identifiziert und realisiert werden, um die Folgen von potenziellen Angriffen auf die leittechnischen Systeme der Anlage zu verhindern oder abzuschwächen.

In Bezug auf die Phasen Operation and Maintenance soll das Risk Assessment periodisch auf den neuesten Stand gebracht werden. Zudem sollte eine Aktualisierung des Risk Assessments erfolgen, wenn neue relevante Schwachstellen erkannt werden oder größere Änderungen der leittechnischen Architektur (z. B. hinzufügen eines Systems, neue Netzwerkverbindungen) erfolgten. Ein Risk Assessment sollte dabei vor jedweden Änderungen, die sich auf die Cybersicherheit auswirken könnten, durchgeführt werden, wobei die Auswirkung auf die Cybersicherheit auf der Grundlage von Risk Assessments betrachtet und vor der Änderung begründet dokumentiert werden sollten.

3.1.3 IEC 61511 „Funktionale Sicherheit – PLT-Sicherheitseinrichtungen für die Prozessindustrie“

Die Norm IEC 61511 “Funktionale Sicherheit – PLT-Sicherheitseinrichtungen für die Prozessindustrie“ /DIN19n01/ befasst sich mit der Anwendung von Sicherheitseinrichtungen der Prozessleittechnik (PLT) in der Prozessindustrie. Zudem behandelt sie die Gefährdungs- und Risikoanalyse der Prozesse, die zur Spezifikation der PLT-Sicherheitseinrichtungen durchzuführen sind. Dabei geht es zunächst um das allgemeine Management im Zusammenhang mit der funktionalen Sicherheit. Bezüglich der in /DIN19n01/ definierten entsprechenden Anforderungen müssen für ein Risikomanagement und ein Risk Assessment Gefährdungen festgestellt, Risiken abgeschätzt und die notwendigen Maßnahmen zur Risiko-Verringerung festgelegt werden. Diesbezüglich im Rahmen des Vorhabens relevante Aspekte werden im Wesentlichen im Kapitel zur Gefährdungs- und Risikobeurteilung des damit verbundenen Prozesses adressiert.

Dabei sind die folgenden Ziele der Anforderungen der Gefährdungs- und Risikobeurteilung des Prozesses definiert, die im Wesentlichen wichtige Schritte, die auch für ein allgemeines Risk Assessment relevant sind, widerspiegeln:

- Ermittlung der Gefährdungen und gefährlichen Vorfälle des Prozesses und der zugehörigen Einrichtungen,
- Ermittlung der Abläufe (Ereigniskette), die hierzu führen können,
- Bestimmung des damit verbundenen Prozessrisikos,
- Aufstellung aller Anforderungen zur Risikominderung,
- Bestimmung erforderlicher Sicherheitsfunktionen zur Erreichung der notwendigen Risikominderung,

- Festlegung, ob sich unter den Sicherheitsfunktionen auch PLT-Sicherheitsfunktionen befinden;

Die dabei definierten Anforderungen erfordern gemäß /DIN19n01/, die oben genannte Gefährdungs- und Risikobeurteilung, für welche die Ergebnisse unter anderem gefährliche Vorfälle und dazu beitragende Faktoren, Eintritts-Wahrscheinlichkeiten und Wahrscheinlichkeiten der Folgewirkungen, Festlegungen von Maßnahmen zur Risikominderung und eine Dokumentation der bei der Risikoanalyse getroffenen Annahmen, umfassen.

In /DIN19n01/ wird explizit auch die Informationssicherheit von Sicherheitseinrichtungen genannt, wobei eine Risikobeurteilung zur Identifikation von Schwachstellen gefordert wird. Diese muss dabei unter anderem eine Beschreibung der abgedeckten Geräte, eine Beschreibung der festgestellten Bedrohungen, die Schwachstellen ausnutzen und zu IT-Sicherheitsvorfällen führen können, eine Beschreibung möglicher Auswirkungen eines IT-Sicherheitsvorfalls und die Auftrittswahrscheinlichkeit, die Feststellung von Anforderungen zur weiteren Verminderung des Risikos und eine Beschreibung der zur Beseitigung oder Verminderung der Bedrohung getroffenen Maßnahmen ergeben. Im Anschluss werden in /DIN19n01/ zudem verschiedene Schutzebenen definiert, zu denen die einzelnen Sicherheitsfunktionen zuzuordnen sind.

3.1.4 IEC 62443 „Industrial communication networks – Network and system security”

Die Norm IEC 62443 “Industrial communication networks – Network and system security“ /IEC09n03/ definiert die Terminologie, Konzepte und Modelle für die Sicherheit von industriellen Automatisierungs- und Steuerungssystemen. In dieser Norm wird unter anderem ein Risk Assessment in Bezug auf potenzielle Bedrohungen beschrieben, welches direkt in mehreren Unterkapiteln bezüglich Assets, Schwachstellen, Risiken und Bedrohungen adressiert wird. Innerhalb dieses Risk Assessments sind gemäß /IEC09n03/ Assets Risiken unterworfen, welche durch den Einsatz von Gegenmaßnahmen, die zur Behebung von Schwachstellen, die von verschiedenen Bedrohungen ausgenutzt werden können, minimiert werden.

Assets werden in /IEC09n03/ in Bezug auf die Sicherung als Fokuselemente, die entsprechend zu schützen sind, betrachtet und können in die Kategorien physisch, logisch und menschlich unterteilt werden.

Demnach ist innerhalb des Risk Assessment zunächst eine Inventarliste der Assets zu erstellen, die schutzbedürftig sind. Nachfolgend geht es um die Bewertung der Assets, wobei der Wert für die Organisation in qualitativen oder quantitativen Größen bemessen sein kann und entsprechende Verluste direkt (beispielsweise Kosten zur direkten Ersetzung des Assets) oder indirekt (zum Beispiel Kosten durch Produktionsausfall) vorliegen können. Die Verluste werden anhand der Kombination aus Informationen über die Art des Assets und dessen Wert kategorisiert. Neben den Assets werden in /IEC09n03/ als nächster Schritt Schwachstellen in Systemen, Komponenten oder Organisationen diskutiert. Für die betrachteten Assets müssen demnach die einzelnen Schwachstellen und damit einhergehenden Risiken betrachtet werden. In einem späteren Kapitel werden in /IEC09n03/ auch Sicherheitszonen und -stufen aufgegriffen, denen die einzelnen Komponenten zugeordnet und die entsprechend der Zone bzw. Stufe abgestuft geschützt werden müssen.

In Bezug auf das Risiko wird in /IEC09n03/ definiert, dass es sich dabei um die Erwartung eines Verlustes handelt auf Grundlage der Wahrscheinlichkeit, dass eine bestimmte Bedrohung eine Schwachstelle ausnutzt und es zu entsprechenden negativen Konsequenzen kommt. Das Risiko wird als Funktion von Bedrohung, Schwachstelle und Auswirkung betrachtet, wobei zu den beiden ersten Faktoren jeweils zugehörige Wahrscheinlichkeiten angegeben werden können, dass eine bestimmte Situation eintritt. Ein Risk Assessment sollte nach /IEC09n03/ alle involvierten Systeme in einem mehrschichtigen Ansatz analysieren, beginnend mit den Systemen, die besonders bedroht sind. Grundlegend werden drei Schritte für ein Risk Assessment genannt:

1. Bewertung des Anfangsrisikos
2. Implementierung von Gegenmaßnahmen zur Abschwächung des Risikos
3. Bewertung des Restrisikos

Die Schritte 2 und 3 werden so oft wiederholt, bis das Restrisiko ein akzeptables Niveau erreicht hat. Die vorgesehenen Gegenmaßnahmen müssen dabei evaluiert und ggf. durch weitere Sicherungsmaßnahmen ergänzt werden. Dabei werden in /IEC09n03/ verschiedene Arten von Risiken genannt, die bei allen Überlegungen berücksichtigt werden müssen: Risiken in Bezug auf die Sicherheit von Personen und Komponenten/Prozessen, Informationssicherheitsrisiken, übergeordnete Risiken beispielsweise in Bezug auf die Einhaltung von Gesetzen und außerdem Business Continuity-Risiken.

Das Ergebnis der in /IEC09n03/ genannten qualitativen Risikoanalyse ist eine Liste von Assets oder Szenarien mit einer zugeordneten Wahrscheinlichkeit in Bezug auf die Risiken und einer Bewertung/Sortierung der jeweiligen Auswirkungen. Hierzu müssen durch das Management angemessene Reaktionen definiert werden, die abhängig vom für die Organisation akzeptablem Restrisiko sind. Diese Reaktionen auf ein Risiko unterteilen sich gemäß /IEC09n03/ in das Ändern des Designs, sodass das Risiko in der Form nicht erhalten ist, die Reduzierung, die Akzeptanz der Transfer des Risikos, sowie die Eliminierung oder Änderung von ineffektiven Maßnahmen, die ein Risiko mitigieren sollen.

In Bezug auf Bedrohungen werden in /IEC09n03/ neben externen und internen Angreifern auch natürliche Bedrohungen wie beispielsweise Erdbeben sowie unwissentliche Vorfälle, die beispielsweise durch unbeabsichtigte menschliche Fehlhandlungen hervorgehen, betrachtet. Zudem wird bezüglich der im Rahmen des Risk Assessments zu betrachtenden Bedrohungen zwischen aktiven und passiven Bedrohungen unterschieden. Als passive Bedrohungen werden dabei im Wesentlichen Informationsbeschaffung und Spionage verstanden, wobei aktive Bedrohungen in /IEC09n03/ Angreiferhandlungen zur Manipulation oder anderweitige maliziöse aktive Handlungen wie Spoofing, Denial-of-Service Angriffe usw. bis hin zu physischer Zerstörung umfassen. In /IEC09n03/ werden außerdem Gegenmaßnahmen in Bezug auf die im Rahmen des Risk Assessments betrachteten Risiken diskutiert, die typischerweise zur Reduzierung eines Risikos eingesetzt werden. Dabei wird zwischen Sicherungsmaßnahmen gegen externe Angreifer wie beispielsweise angemessene Access Controls und Authentifizierungen, Verschlüsselung und auch physischen Sicherungsmaßnahmen sowie Sicherungsmaßahmen in Bezug auf interne und passive Bedrohungen unterschieden.

3.1.5 ISO 31000 – „Risikomanagement – Leitlinien“

Die ISO 31000 „Risikomanagement – Leitlinie“ /ISO18n04/ ist eine Norm, die sich explizit mit dem Thema Risiko-Management beschäftigt und dabei explizit auf die damit einhergehenden einzelnen Aspekte eingeht. Der Prozess des Risiko-Managements wird detailliert beschrieben und die einzelnen Schritte individuell diskutiert. Die Norm richtet sich dabei an Personen, die für ihre Organisationen mit Risiken umgehen, Entscheidungen treffen, Ziele festlegen und erreichen sowie Leistungen verbessern sollen. Im Folgenden werden die für das Vorhaben wesentlichen Inhalte zusammengefasst.

Zunächst werden in /ISO18n04/ Grundsätze in Bezug auf die Eigenschaften eines effizienten, wirksamen Risikomanagements definiert. Demnach sollte das Risiko-Management ein integraler Bestandteil aller Aktivitäten einer Organisation sein und dabei strukturiert, umfassend und maßgeschneidert durchgeführt werden, um konsistente und vergleichbare Ergebnisse zu erzielen und den externen und internen Kontext einer Organisation zu berücksichtigen. Dabei sollten alle relevanten Parteien rechtzeitig eingebunden werden und Risiken sollten dynamisch erfasst und entsprechend behandelt werden. Die Grundlage aller Entscheidungen bilden zudem zeitgerecht verfügbare, verständliche Informationen, die allen relevanten Parteien zur Verfügung stehen. Schließlich müssen menschliche und kulturelle Faktoren berücksichtigt werden und der Prozess sollte durch Lernen und Erfahrung fortlaufend verbessert werden. Diese Grundsätze sollten gemäß /ISO18n04/ im Rahmen des Risikomanagements berücksichtigt werden und die Grundlage für den Umgang mit Risiken bilden. In Bezug auf die Integration des Risikomanagements in die relevanten Aktivitäten und Funktionen wird in /ISO18n04/ ein Rahmenwerk beschrieben, das die Organisation dabei entsprechend unterstützen soll. Dieses umfasst die Integration, Gestaltung, Implementierung, Bewertung und Verbesserung des Risikomanagements, wobei die einzelnen Aspekte jeweils ausführlich diskutiert werden.

Im Rahmen des Vorhabens sind insbesondere die Abschnitte zum Risikomanagement-Prozess relevant. Dieser ist in Abb. 3.1 mit den einzelnen Schritten und deren Zusammenhängen zueinander veranschaulicht. Dieser Prozess sollte in die Struktur, Abläufe und Prozesse der Organisation integriert werden und Bestandteil des Managements, sowie der Entscheidungsfindung sein. Der Risikomanagementprozess ist ein iterativer Prozess. Im Folgenden werden die in Abb. 3.1 dargestellten für das Vorhaben relevanten Inhalte, die in /ISO18n04/ beschrieben werden, zusammengefasst.

Zunächst ist es wichtig, die relevanten Parteien durch durchgehende Kommunikation und Konsultation in Bezug auf die Risiken, die Entscheidungsgrundlagen und Gründe für bestimmte erforderliche Aktionen zu informieren und einzubinden. Dies dient unter anderem einerseits zur Förderung des Risikobewusstseins und andererseits zur Erlangung von Feedback und Informationen in Bezug auf die Entscheidungsfindung. Eine angemessene Kommunikation und Konsultation ist dabei vor allem relevant, um Fachkenntnisse aus verschiedenen Bereichen zu vereinen und sicherzustellen, dass verschiedene Sichtweisen und Ansichten beim Risk Assessment berücksichtigt werden.

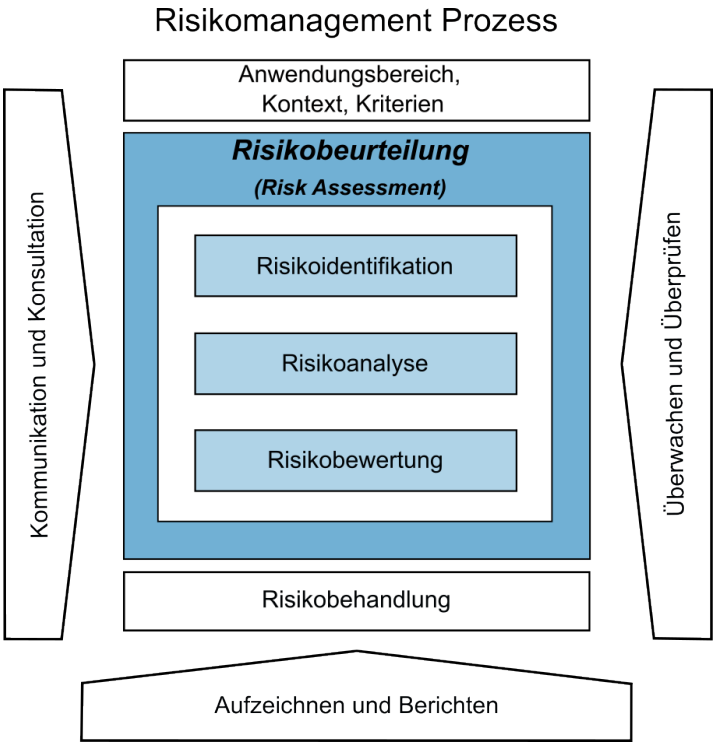

Abb. 3.1 Schritte des Risikomanagement Prozesses und Einordnung des Risk Assessments mit den einzelnen Schritten gemäß ISO 31000

Ein weiterer wichtiger Aspekt ist die Kontextualisierung. Für eine wirksame Risikobeurteilung und eine geeignete Risikobehandlung sollten der Anwendungsbereich, der interne und externe Kontext, sowie die Risikokriterien entsprechend festgelegt werden. Dabei geht es im Wesentlichen um eine Bestimmung der Ziele, der erforderlichen Ressourcen und Verantwortlichkeiten und verschiedene technische Einzelheiten, die im Rahmen des Risiko-Managements relevant sind. Dazu zählen beispielsweise Fragen in Bezug auf die Festlegung von Auswirkungen und Wahrscheinlichkeiten oder in Bezug auf die Frage, auf welche Art und Weise Charakteristika wie Risikohöhen bestimmt werden.

Ein wesentlicher Teil des in /ISO18n04/ beschriebenen Prozesses ist die Risikobeurteilung bzw. das Risk Assessment. In dieser Norm bezeichnet der Begriff „Risikobeurteilung“ den gesamten Prozess der Risikoidentifizierung, Risikoanalyse und Risikobewertung. Die Risikobeurteilung sollte demnach systematisch, iterativ und kollaborativ unter Nutzung der Kenntnisse und Ansichten der beteiligten Parteien durchgeführt werden und die bestmöglichen verfügbaren Informationen berücksichtigen.

Im Rahmen der Risikoidentifizierung sollen für die Organisation relevante Risiken anhand geeigneter und aktueller Informationen erkannt und beschrieben werden. Zur Identifizierung von Unsicherheiten, die Auswirkungen auf eines oder mehrere Ziele haben können, können gemäß /ISO18n04/ verschiedene Verfahren angewandt werden. Dazu werden in der Norm wichtige Faktoren genannt, die entsprechend bei der Risikoidentifizierung berücksichtigt werden sollten. Diese umfassen unter anderem materielle und immaterielle Risikoquellen, Bedrohungen, Schwachstellen, Indikatoren für aufkommende Risiken und relevante Auswirkungen. Bei der Identifizierung von Risiken ist es dabei unerheblich, ob deren Ursachen im Einflussbereich einer Organisation liegen oder nicht.

Bei der Risikoanalyse besteht der Zweck darin, die Art des Risikos, sowie die Eigenschaften und gegebenenfalls die Risikohöhe zu verstehen. Bei Risikoanalysen werden Unsicherheiten, Risikoursachen, Auswirkungen, Wahrscheinlichkeiten, Ereignisse, Szenarien, Steuerungen und deren Wirksamkeit ausführlich betrachtet. Die Risikoanalyse kann dabei unterschiedlich detailliert oder komplex sein, abhängig vom Zweck der Analyse, der Verfügbarkeit und Verlässlichkeit der Informationen, sowie der verfügbaren Ressourcen. Abhängig von den Umständen und der vorgesehenen Nutzung können die Analysetechniken qualitativ, quantitativ oder eine Kombination der beiden sein. Auch im Zusammenhang mit der Risikoanalysen werden in /ISO18n04/ Faktoren genannt, die entsprechend berücksichtigt werden sollen. Diese umfassen unter anderem Wahrscheinlichkeiten von Ereignissen und Auswirkungen sowie deren Art und Umfang, zeitliche Faktoren sowie Überlegungen zur Wirksamkeit bestehender Maßnahmen. Es gibt dabei gemäß /ISO18n04/ zahlreiche Einflussfaktoren einer Risikoanalyse wie beispielsweise getroffene Annahmen, die berücksichtigt, dokumentiert und kommuniziert werden sollten. Für sehr ungewisse Ereignisse bietet sich eine Kombination aus verschiedenen Verfahren an, wenn eine Quantifizierung schwierig ist und zu Unsicherheiten bei der Analyse von Ereignissen mit schwerwiegenden Auswirkungen führt. Ein wichtiges Ergebnis der Risikoanalyse sind Entscheidungshilfen hinsichtlich der Risikobewertung, insbesondere in Bezug auf die Fragen, ob und wie Risiken zu behandeln sind und welche Strategien und Methoden der Risikobehandlung für diese am besten geeignet sind.

Als letzter Teil des eigentlichen Risk Assessments dient die Risikobewertung zur Unterstützung bei Entscheidungen, indem Ergebnisse aus der Risikoanalyse mit den festgelegten Risikokriterien verglichen werden, um zu analysieren, an welcher Stelle zusätzliche Aktionen erforderlich sind. Darauf aufbauend können unter anderem unterschiedliche Entscheidungen getroffen werden:

- keine weiteren Maßnahmen,
- Erwägung von Optionen zur Risikobehandlung,
- Durchführung weiterer Analysen zum besseren Verständnis des Risikos,
- Anpassung der Ziele;

Dabei ist es gemäß /ISO18n04/ wichtig, das Ergebnis der Risikobewertung aufzuzeichnen, zu kommunizieren und zu validieren.

Als nächstes geht es in /ISO18n04/ um die Risikobehandlung. Diese dient dabei zur Auswahl und Implementierung von Optionen zur Behandlung des Risikos. Dieser iterative Prozess beinhaltet unter anderem das Auswählen geeigneter Optionen, das Planen und Implementieren der Risikobehandlung, das Beurteilen der Wirksamkeit der Behandlung sowie die Entscheidung, ob das verbleibende Risiko akzeptabel ist, und ggf. das Vornehmen weiterer Behandlungen. Die Grundlage der Auswahl von Maßnahmen zur Risikobehandlung bilden gemäß /ISO18n04/ Abwägungen zwischen potenziell erzielten Vorteilen durch das Erreichen der Ziele, gegen die Kosten, den Aufwand oder die Nachteile der Implementierung. Die Möglichkeiten zur Behandlung von Risiken können zudem unter anderem grundlegend eine oder mehrere der folgenden Optionen umfassen: Vermeidung von Risiken, Beseitigung der Risikoursache, Veränderung der Eintrittswahrscheinlichkeit oder der Auswirkungen, sowie Transfers oder Beibehaltung des Risikos. Dabei gilt es zu beachten, dass die Behandlung von Risiken zu neuen Risiken führen kann und geplante Maßnahmen ggf. nicht zu den erwarteten Ergebnissen führen. Daher sollte die Überwachung und Überprüfung einen integralen Bestandteil bei der Implementierung der Risikobehandlung darstellen, um die Wirksamkeit der Risikobehandlung sicherzustellen.

Die Qualität und Wirksamkeit des Prozesses soll durch das **Überwachen und Überprüfen** sichergestellt und verbessert werden. Dies sollte laufend und regelmäßig in allen Phasen des Prozesses erfolgen und ein geplanter Teil des Risikomanagementprozesses mit eindeutig festgelegten Verantwortlichkeiten sein.

Als letzter Schritt geht es in /ISO18n04/ um das Aufzeichnen und Berichten. Eine Dokumentation der Ergebnisse des Risikomanagementprozesses, sowie der Prozess an sich ist essenziell.

3.1.6 IEC 31010 „Risikomanagement – Verfahren zur Risikobeurteilung“

Die Norm IEC 31010 Standard „Risikomanagement – Verfahren zur Risikobeurteilung“ /IEC19n04/ bietet Informationen in Bezug auf die Auswahl und Anwendung verschiedener Techniken, die zur Unterstützung des Risiko-Managements verwendet werden können. Diese Techniken werden innerhalb der unter anderem in der ISO 31000 beschriebenen Schritte des Risk Assessments (Risikoidentifizierung, Risikoanalyse, Risikobewertung) angewendet. Insgesamt ist dabei neben dem Umgang mit Risiken insbesondere die Betrachtung von Unsicherheiten ein wesentlicher Fokusbereich der Norm. Im Wesentlichen befasst sich die Norm mit der Nutzung, Implementierung und Auswahl von Risk Assessment Techniken und bietet außerdem eine Übersicht und Kategorisierung ausgewählter Techniken. Im Folgenden werden die für das Vorhaben relevanten Inhalte kurz zusammengefasst.

In Bezug auf die Nutzung der in /IEC19n04/ diskutierten Risk Assessment Techniken wird zunächst spezifiziert, unter welchen Umständen die Nutzung erfolgen sollte. Dies ist beispielsweise der Fall, wenn tieferes Verständnis über die existierenden Risiken oder ein bestimmtes Risiko erforderlich ist oder generell im Rahmen von Risiko-Management- bzw. Entscheidungsprozessen. Die Art und Weise, wie das Risiko bewertet wird, hängt nach /IEC19n04/ von der Komplexität und Neuartigkeit der Situation, sowie vom Niveau des relevanten Wissenstandes und Verständnisses ab. Als einfachster Fall wird als Beispiel eine bereits bekannte Situation genannt, bei der die Risiken gut verstanden sind und keine signifikanten Konsequenzen aufweisen. Maßnahmen werden in diesem Fall üblicherweise gemäß den etablierten Regeln und Prozeduren, sowie anhand vorheriger Assessments von Risiken beschlossen. Für neue, komplexe oder auch anspruchsvolle Situationen, bei denen es eine hohe Unsicherheit und wenig Erfahrungen gibt, sind die Informationen, auf denen die Entscheidung gestützt wird, gering und konventionelle Techniken der Analyse wahrscheinlich nicht nützlich oder sinnvoll. Als Gegenbeispiel zum ersten Fall sollten gemäß /IEC19n04/ in diesen Fällen verschiedene Techniken angewendet werden, um ein partielles Verständnis der Risiken zu erreichen, wobei die Beurteilungen dann unter anderem im Kontext der organisatorischen und gesellschaftlichen Werte erfolgt.

Die Implementierung des Risk Assessments unterteilt sich gemäß /IEC19n04/ zunächst grundsätzlich in die Schritte Planung, Auswertung der Informationen und Entwicklung von Modellen, Anwendung der Risk Assessment Techniken, Überprüfung der Analysen und Verwendung der Ergebnisse zur Unterstützung der Entscheidungen. Für die Planung eines Assessments sind dabei unter anderem insbesondere die Definition der Ziele und des Umfangs des Risk Assessments sowie ein Verständnis des Kontextes relevant. Als Vorbereitung für das Risk Assessment und währenddessen sollten gemäß /IEC19n04/ die relevanten Informationen ermittelt werden. Diese Informationen werden für statistische Analysen, Modelle oder andere Techniken verwendet. Zunächst ist demnach in Bezug auf das Sammeln der Informationen unter anderem insbesondere zu entscheiden, welche Quellen verwendet werden, welche Art Informationen relevant sind und wie diese gesammelt werden sollen. Die weiteren in /IEC19n04/ beschriebenen Schritte umfassen das Analysieren der erhobenen Daten sowie die Entwicklung und Anwendung von darauf aufbauenden Modellen.

Ein Großteil der Diskussion bezüglich der Implementierung eines Risk Assessment in /IEC19n04/ befasst sich mit der Anwendung von konkreten Risk Assessment Techniken. Diese können demnach zur Risikoidentifizierung, Ermittlung der Risikoursachen und -quellen, Untersuchung der Wirksamkeit von Maßnahmen, Verständnis der Konsequenzen und der entsprechenden Wahrscheinlichkeiten, Analyse der Wechselwirkungen und Abhängigkeiten und der Festlegung eines Vergleichsmaßstabs zur Einschätzung eines Risikos genutzt werden. Im Folgenden werden die einzelnen Aspekte kurz zusammengefasst.

Zur Identifizierung von Risiken werden gemäß /IEC19n04/ typischerweise Techniken verwendet, die auf bekanntes Wissen und Erfahrungen zurückgreifen. Diese Techniken berücksichtigen unter anderem welche Unsicherheiten existieren und welche Auswirkungen daraus resultieren könnten, welche Risikoquellen existieren oder sich entwickeln könnten, welche Maßnahmen bereits etabliert sind und wie effektiv diese sind, was für potenzielle Auswirkungen auftreten können und welche relevanten Ereignisse bereits in der Vergangenheit aufgetreten sind und wie diese ggf. Auswirkungen auf die Zukunft haben könnten. Bei den Ergebnissen der Risikoidentifizierung handelt es sich demnach beispielsweise um eine Auflistung der Risiken mit den entsprechend relevanten Ereignissen, Ursachen und spezifizierten Auswirkungen. Obwohl Risiken möglichst früh identifiziert werden sollten, um möglichst zeitnah entsprechende Maßnahmen ergreifen zu können, wird in /IEC19n04/ erläutert, dass einige Risiken ggf. im Laufe des Risk

Assessments nicht direkt identifiziert werden können, sodass ein Verfahren zur Verfügung etabliert sein sollte, dass es ermöglicht neu aufgetretene Risiken zu erfassen. Konkrete Techniken Risikoidentifizierung werden in /IEC19n04/ zudem in einem der Anhänge beschrieben.

In Bezug auf die Ermittlung von Risikoursachen und -quellen geht es gemäß /IEC19n04/ zunächst unter anderem darum, Einschätzungen bezüglich der Eintrittswahrscheinlichkeit eines Ereignisses oder einer Auswirkung besser durchführen zu können, Handlungsmöglichkeiten in Bezug auf die Risiken zu identifizieren und Indikatoren bezüglich möglicherweise auftretender Probleme zu ermitteln. Risikoursachen und -quellen können demnach beispielsweise Ereignisse, Entscheidungen, Handlungen und Prozesse sein. Konkrete Techniken zur Ermittlung von Risikoursachen und -quellen werden in /IEC19n04/ zudem in einem der Anhänge beschrieben.

Im nächsten Schritt werden in /IEC19n04/ Untersuchungen in Bezug auf die Wirksamkeit von Maßnahmen zum Umgang mit Risiken diskutiert. Demnach ist insbesondere zu betrachten, ob die eingesetzten Maßnahmen wie beabsichtig funktionieren und die erwarteten Ergebnisse erzielen, ob es Defizite in der Auslegung der Maßnahmen gibt oder bei der Art und Weise wie sie angewendet werden, ob die Maßnahmen unabhängig voneinander funktionieren oder ob diese kollektiv arbeiten müssen, um wirksam zu sein, ob es Faktoren, Bedingungen, Schwachstellen oder Umstände gibt, die die Wirksamkeit der Maßnahmen reduzieren oder aufheben können und ob Maßnahmen zusätzliche Risiken hervorrufen können. Dabei sollte jede Annahme, die während des Risiko Assessments über die tatsächliche Wirksamkeit und Zuverlässigkeit von Maßnahmen getroffen wird, wenn möglich validiert werden. Konkrete Techniken zur Untersuchung der Wirksamkeit von Maßnahmen werden in /IEC19n04/ zudem in einem der Anhänge beschrieben.

In Bezug auf das Verständnis der Konsequenzen und der entsprechenden Wahrscheinlichkeiten im Zusammenhang mit den betrachteten Risiken kann eine Analyse gemäß /IEC19n04/ von der Beschreibung bestimmter Ergebnisse bis hin zu detaillierten quantitativen Modellen oder Schwachstellenanalysen variieren. Risiken können demnach weiterhin mit einer Vielzahl von unterschiedlichen Auswirkungen assoziiert werden, die sich wiederum auf verschiedene Ziele auswirken können. Der festgelegte Kontext sollte dabei überprüft werden, sodass sichergestellt ist, dass die zu analysierenden Auswirkungen mit dem Ziel des Risk Assessments und den zu treffenden Entscheidungen zusammenpassen. Das Ausmaß der Auswirkungen kann gemäß /IEC19n04/ quantitativ beispielsweise als spezifischer Wert ausgedrückt werden oder als Verteilung, wenn einer

Auswirkung kein fester Wert zugeordnet werden kann, wenn die Auswirkungen abhängig von den Randbedingungen variieren oder variierende Parameter die Auswirkung beeinflussen. Die Wahrscheinlichkeit kann sich im Rahmen von /IEC19n04/ auf die Eintrittswahrscheinlichkeit eines Ereignisses oder einer spezifischen Auswirkung beziehen. Der Parameter, für den eine Wahrscheinlichkeit gilt, sollte demnach entsprechend explizit angeben werden und das Ereignis oder die Auswirkung, deren Eintrittswahrscheinlichkeit angegeben wird, klar und genau definiert sein. Die Wahrscheinlichkeit kann gemäß /IEC19n04/ auf verschiedene Arten beschrieben werden, einschließlich quantitativ als erwartete Wahrscheinlichkeit oder Häufigkeit oder qualitativ durch genau zu definierende beschreibende Begrifflichkeiten (wie beispielsweise „sehr wahrscheinlich“). Konkrete Techniken in Bezug auf das Verständnis der Konsequenzen und der entsprechenden Wahrscheinlichkeiten im Zusammenhang mit den betrachteten Risiken werden in /IEC19n04/ zudem in einem der Anhänge beschrieben.

Im nächsten Schritt werden in /IEC19n04/ Wechselwirkungen und Abhängigkeiten betrachtet. Demnach gibt es typischerweise viele Wechselwirkungen und Abhängigkeiten zwischen Risiken. Beispielsweise können zahlreiche Auswirkungen aus einer einzelnen Ursache entstehen oder eine bestimmte Auswirkung kann unterschiedliche Ursachen haben. Zudem kann das Auftreten von einigen Risiken das Auftreten anderer Risiken begünstigen oder verhindern. Um dies zu berücksichtigen und ein zuverlässigeres Risk Assessments durchzuführen, bei dem die kausalen Zusammenhänge zwischen den Risiken berücksichtigt werden, kann es gemäß /IEC19n04/ nützlich sein ein kausales Modell zu erstellen, welches diese Risiken einbezieht. Hierzu werden unter anderem konkrete Techniken in Bezug auf die Analyse Wechselwirkungen und Abhängigkeiten in /IEC19n04/ in einem der Anhänge beschrieben.

In Bezug auf die Festlegung eines Vergleichsmaßstabs zur Einschätzung eines Risikos ist es gemäß /IEC19n04/ in manchen Situationen sinnvoll, die Bewertung als Kombination des Ausmaßes der potenziellen Konsequenzen und der Eintrittswahrscheinlichkeit dieser Konsequenzen vorzunehmen. Dabei kann ein qualitativer, semi-quantitativer oder quantitativer Ansatz gewählt werden. Qualitative Ansätze basieren dabei typischerweise auf deskriptiven oder bewertenden Skalen der Auswirkungen und deren Eintrittswahrscheinlichkeit, wohingegen quantitative Ansätze auf die Bewertung von Auswirkungen und Wahrscheinlichkeiten setzen, die auf numerischen Skalen ausgedrückt werden. Semi-quantitative Ansätze umfassen grundsätzlich qualitative und quantitative Aspekte.

In Bezug auf die Vergleichbarkeit gibt es gemäß /IEC19n04/ unterschiedliche Faktoren zu berücksichtigen. Werden beispielsweise quantitative Abschätzungen der Auswirkungen und der Eintrittswahrscheinlichkeit als simples Produkt kombiniert, um das Ausmaß eines Risikos zu erhalten, können Informationen verloren gehen. Zur Kompensation kann in solchen Fällen beispielsweise ein Gewichtungsfaktor für die Auswirkungen oder die Eintrittswahrscheinlichkeit verwendet werden. Bei qualitativen oder semi-quantitativen Ansätzen muss sichergestellt sein, dass die Methodiken, Annahmen und gewählten Größen vergleichbar sind.

Als nächster übergeordneter Schritt wird in /IEC19n04/ die Überprüfung der in den vorherigen Schritten durchgeführten Analysen diskutiert. Dabei geht es zunächst grundsätzlich darum, die Ergebnisse zu verifizieren und zu validieren. Die Verifizierung beinhaltet dabei die Überprüfung, ob die Analyse richtig durchgeführt wurde. Die Validierung umfasst die Überprüfung, ob die richtige Analyse verwendet wurde, um die gesetzten Ziele zu erreichen. Ein weiterer relevanter Aspekt, der in /IEC19n04/ in diesem Zusammenhang adressiert wird, betrifft die Unsicherheit und Sensitivität der Analysen. Unsicherheiten in einer Analyse können aus unterschiedlichen Gründen entstehen und müssen entsprechend berücksichtigt werden. Zudem kann eine Sensitivitätsanalyse verwendet werden, um die Signifikanz von Unsicherheiten in den Daten oder den Annahmen der zugrundeliegenden Analyse zu bewerten. Sensitivitätsanalysen beinhalten dabei die Ermittlung der relativen Veränderung der Ergebnissen, hervorgerufen durch die Änderung von einzelnen Eingabeparametern. Alle relevanten Prozesse, Analysen und sonstige mit dem Risk Assessment verbundenen Aktivitäten sollten permanent bzw. periodisch überwacht und überprüft werden, beispielsweise um das Auftreten von Änderungen schnellstmöglich zu identifizieren und um ggf. neue Informationen oder neue Methoden angemessen zu berücksichtigen.

Der letzte Aspekt, der in /IEC19n04/ diskutiert wird, betrifft im Wesentlichen die Verwendung der Ergebnisse zur Unterstützung der zu treffenden Entscheidungen. Demnach leisten die Ergebnisse einer Risikoanalyse einen Beitrag zum Treffen von Entscheidungen über mögliche Handlungen. Die Faktoren, die bei einer Entscheidungsfindung beachtet werden sollten und die spezifischen Kriterien, die zu berücksichtigen sind, sollten gemäß /IEC19n04/ am Anfang eines Assessments bei der Erstellung des Assessment Kontext definiert werden. Dabei wird in /IEC19n04/ zwischen zwei Arten relevanter Entscheidungen unterschieden: Entscheidungen über die Bedeutung, Signifikanz und ggf. Behandlung von einzelnen Risiken und Entscheidungen im Zusammenhang mit dem

Vergleich zwischen verschiedenen zur Verfügung stehenden Optionen in Bezug auf entsprechende Risiken. Hierzu werden unter anderem konkrete Techniken in Bezug konkrete Vorgehensweisen in diesem Zusammenhang in /IEC19n04/ in einem der Anhänge beschrieben.

Abschließend geht es in /IEC19n04/ um die Dokumentation und Zusammenfassung des Risk Assessment Prozesses und der Resultate. Die Ergebnisse, die verwendeten Methoden und die Begründung der Annahmen, sowie die Empfehlungen sollten entsprechend dokumentiert werden. Zudem sollte entschieden werden, welche Informationen in welcher Form kommuniziert werden und mit wem.

3.1.7 ISO 2700x Normenreihe

Die ISO 2700x Normenreihe befasst sich mit der Organisation der Informationssicherheit in Zusammenhang mit einem Informationssicherheitsmanagementsystem (ISMS). Im Folgenden werden für dieses Vorhaben relevante Teile der Normenreihe kurz vorgestellt.

3.1.7.1 ISO 27001 – „Informationssicherheitsmanagementsysteme - Anforderungen“

Die Norm ISO 27001 „Informationssicherheitsmanagementsysteme – Anforderungen“ /ISO17n02/ legt die Anforderungen für die Einrichtung, Umsetzung, Aufrechterhaltung und fortlaufende Verbesserung eines Informationssicherheitsmanagementsystems im Kontext einer Organisation fest. Darüber werden Anforderungen für die Beurteilung und Behandlung von Informationssicherheitsrisiken adressiert. In Bezug auf das ISMS werden in /ISO17n02/ die Punkte Führung, Planung, Unterstützung, Betrieb, Bewertung der Leistung und Verbesserung diskutiert, wobei insbesondere die ersten beiden Punkte für das Vorhaben relevant sind.

Dabei geht es zunächst im Zusammenhang mit der Führung bzw. obersten Leitung um Aufgaben und Verpflichtungen in Bezug auf ISMS, wie beispielsweise die entsprechende organisatorische Verankerung innerhalb der Organisation, die Festlegung der Ziele sowie Rollen, Verantwortlichkeiten und Befugnisse. Konkrete Bezüge zum Thema Risiko-Management bzw. dem Umgang mit Risiken folgen im Abschnitt zur Planung.

Demnach muss die Organisation bei der Planung des ISMS unter anderem Risiken und Chancen bestimmen, um sicherzustellen, dass die durch das ISMS beabsichtigten Ergebnisse erzielt werden können und somit unerwünschte Auswirkungen verhindert oder verringert und fortlaufende Verbesserungen erreicht werden können. Die Organisation muss gemäß /ISO17n02/ die Maßnahmen zu diesen Risiken und Chancen, sowie die Integrierung und Umsetzung dieser Maßnahmen in die Prozesse, planen und eine Bewertung der Wirksamkeit muss auch in der Planung bedacht werden. Unter den Schritt der Planung fällt in /ISO17n02/ insgesamt die Risikobeurteilung (Risk Assessment), die Risikobehandlung und Überlegungen zur Erreichung der Ziele der Informationssicherheit.

Im Rahmen des Risk Assessments muss gemäß /ISO17n02/ ein Prozess zur Beurteilung des Informationssicherheitsrisikos festgelegt und angewendet werden. Dabei werden in dieser Norm Anforderungen an den Prozess definiert, denen das Risk Assessment genügen muss. Diese umfassen unter anderen die Festlegung von Kriterien zur Beurteilung von Risiken und der Risikoakzeptanz, sowie die Identifizierung, Analyse und Bewertung von Informationssicherheitsrisiken. Im Rahmen des in /ISO17n02/ geforderten Prozesses zur Risikobehandlung geht es unter anderem darum, Handlungsoptionen unter Berücksichtigung der Ergebnisse des Risk Assessments auszuwählen, Maßnahmen zur Umsetzung festzulegen und Überlegungen zur Anwendbarkeit anzustellen. In Bezug auf die Überlegungen zur Erreichung der Ziele der Informationssicherheit geht es in /ISO17n02/ im Wesentlichen um die Festlegung von Zielen für relevante Funktionen und Ebenen, sowie die Dokumentation zugehöriger Informationen und Planung der zur Erreichung nötigen Schritte (beispielsweise notwenige Ressourcen, Verantwortlichkeiten etc.).

3.1.7.2 ISO 27002 – „Auswahl von Maßnahmen“

Die Norm ISO 27002 /ISO17n03/ fokussiert sich aufbauend auf der ISO 27001 im Wesentlichen auf die Auswahl, Implementierung und Anwendung von Sicherungsmaßnahmen im Rahmen der jeweiligen Risikoumgebung der Informationssicherheit einer Organisation. Dabei geht es zunächst im Wesentlichen darum konkrete Sicherungsanforderungen identifizieren. Dazu wird in /ISO17n03/ unter anderem ein Risk Assessment für die Organisation, welches die Unternehmensstrategie und die Ziele der Organisation mit einbezieht, als Hauptquelle für Sicherungsanforderungen an die Informationssicherheit genannt.

Während dieses Prozesses werden relevante Bedrohungen identifiziert, Schwachstellen und zugehörige Eintrittswahrscheinlichkeit sowie das Ausmaß des Eintretens eines Risikos bewertet, was für die oben genannte Auswahl, Implementierung und Anwendung von Sicherungsmaßnahmen essenziell ist. Die Ergebnisse des Risk Assessments helfen gemäß /ISO17n03/ dabei die Handlungen der entscheidungsberechtigten Parteien zu bestimmen, sowie Prioritäten zu setzen und mit den Risiken der Informationssicherheit angemessen umzugehen.

Insgesamt werden in /ISO17n03/ 114 Sicherungsmaßnahmen in 35 Kategorien wie beispielsweise Kommunikationssicherheit, Informationssicherheitsvorfalls-Management oder Business Continuity aufgeführt. Jede Kategorie beinhaltet dabei ein Ziel, welches erreicht werden soll und eine oder mehrere Maßnahmen, die angewendet werden können, um dieses Ziel zu erreichen. Dabei werden neben der spezifischen Maßnahmen jeweils detaillierte Informationen zur Implementierung und zur Erreichung des Ziels zur Verfügung gestellt. Zudem werden weitere Informationen zur Verfügung gestellt, die möglicherweise beachtet werden müssen, wie beispielsweise rechtliche Betrachtungen und Hinweise für andere Standards. Für das Vorhaben ist somit insbesondere der Zusammenhang der Sicherungsmaßnahmen angesichts der identifizierten Risiken relevant.

3.1.7.3 ISO 27005 – „Informationssicherheitsmanagement“

Die ISO 27005 /ISO18n03/ bietet eine Leitlinie zum Risk Management für die Informationssicherheit. Die Norm unterstützt das generelle Konzept, welches in der ISO 27001 spezifiziert ist, indem Empfehlungen für die Implementierung basierend auf einem Risikomanagementansatz anhand konkreter Inhalte gegeben werden. Das Wissen über die Konzepte, Modelle, Prozesse, sowie der Terminologie aus der ISO 27001 und ISO 27002 sind relevant für ein Verständnis dieses Dokuments.

Der Risikomanagement-Prozess für die Informationssicherheit setzt sich gemäß /ISO18n03/ im Wesentlichen aus der Erstellung des Kontextes, dem Risk Assessment und der Risikobehandlung zusammen. Die Zusammenhänge der einzelnen Schritte bzw. Punkte sind in Abb. 3.2 veranschaulicht und werden im Folgenden kurz zusammengefasst. Zunächst sollten im Rahmen der Erstellung des Kontextes alle Informationen über die Organisation, die relevant für das Informationssicherheitsrisikomanagement sind, verwendet werden.

Relevant für den Kontext ist unter anderem die Festlegung relevanter Kriterien, die Definition des Umfangs sowie die Festlegung des Zwecks und der Ziele. Letzteres kann gemäß /ISO18n03/ beispielsweise die Unterstützung des Managementsystems für Informationssicherheit (Information Security Management System, ISMS) oder die Einhaltung geltender Rechtsvorgaben und der Nachweis der Sorgfaltspflicht sein. Unter die relevanten Kriterien fallen in diesem Zusammenhang beispielsweise Kriterien für die Risikobewertung, die Auswirkung und die Risikoakzeptanz. Der Umfang des Prozesses muss im Wesentlichen definiert werden, um sicherzustellen, dass alle relevanten Aspekte berücksichtigt werden.

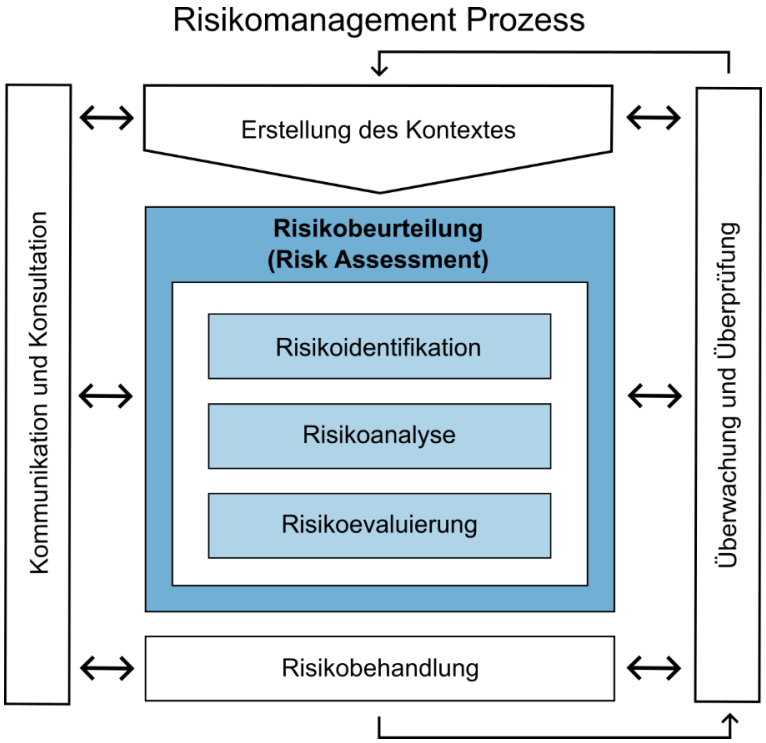

Abb. 3.2 Schritte des Risikomanagement-Prozesses und Einordnung des Risk Assessments mit den einzelnen Schritten laut ISO 27005

Der zentrale Bestandteil des Risikomanagement-Prozesses ist das Risk Assessment. Dabei sollten die im vorigen Schritt betrachteten Kriterien, der definierte Umfang und die gesetzten Ziele entsprechend berücksichtigt werden. Das Risk Assessment quantifiziert oder beschreibt qualitativ Risiken und ermöglicht Entscheidungsträgern das Risiko nach deren wahrgenommener Schwere oder anderen erstellten Kriterien zu priorisieren.

Im Rahmen eines Risk Assessments werden allgemein unter anderem relevante Bedrohungen und Schwachstellen identifiziert, Maßnahmen und deren Wirkung in Bezug auf das identifizierte Risiko betrachtet, und potenzielle Auswirkungen bestimmt. Dazu werden Risk Assessments für gewöhnlich mehrmals durchgeführt, wobei zunächst ein Risk Assessment für hohe Risiken durchgeführt wird. Dies dient zur Identifizierung der potenziell größten Risiken. Die anschließende Iteration kann weitere, tiefer gehende Überlegungen beinhalten, die auch die vorherigen Iteration berücksichtigen. Das Ergebnis sollte eine Liste der bewerteten Risiken sein, die nach den Risikobewertungskriterien geordnet sind. Das Risk Assessment beinhaltet gemäß /ISO18n03/ eine Risiko-Identifizierung, eine Risiko-Analyse und eine Risiko-Evaluierung. Diese Schritte werden im Folgenden kurz diskutiert.

Das Ziel der Risiko-Identifizierung ist die Bestimmung, welche Risiken einen potenziellen Verlust verursachen können, sowie Erkenntnisse zu den genauen Umständen zu gewinnen. Eine Risikoidentifizierung umfasst im Wesentlichen Schritte zur Identifizierung der Assets, der Bedrohungen, der bereits existierenden Maßnahmen in diesem Zusammenhang, der potenziellen Schwachstellen, und der möglichen Auswirkungen.

Kernstück des Risk Assessments ist die Risikoanalyse. Diese kann in unterschiedlichen Detailierungsgraden durchgeführt werden abhängig von der Kritikalität der Assets, dem Umfang der bekannten Schwachstellen oder anderer relevanter Kriterien. Die Methodik kann dabei qualitativ oder quantitativ oder eine Kombination sein. Eine qualitative Risikoanalyse verwendet dabei eine Skala mit qualitativen Attributen zur Beschreibung der Stärke potenzieller Auswirkungen (wie niedrig, mittel und hoch) und der Wahrscheinlichkeit, dass diese Auswirkungen auftreten werden. Bei der quantitativen Risikoanalyse wird eine Skala mit nummerischen Werten für die Auswirkungen und die Wahrscheinlichkeiten verwendet, basierend auf Daten aus einer Vielzahl von Quellen. Wesentliche Faktoren im Rahmen der Risikoanalyse sind die Bewertung der möglichen Auswirkungen, der jeweiligen Eintrittswahrscheinlichkeiten und die Ermittlung der Stufe der jeweiligen Risiken.

Grundlage der Risiko-Evaluierung ist eine Liste der zuvor analysierten Risiken mit den zugeordneten Risikostufen. Daran ansetzend wird die Risikostufe mit den im Rahmen der Kontextualisierung diskutierten Kriterien und Akzeptanzkriterien betrachtet. Die Entscheidungen im Rahmen der Risiko-Evaluierung basieren hauptsächlich darauf, welche Risikostufe als akzeptabel eingestuft wird.

Dabei wird das im Rahmen der Risiko-Analyse erlangte Verständnis und Erkenntnisse in Bezug auf die Risiken genutzt, um Entscheidungen über zukünftige Handlungen zu treffen. Durch die Risiko-Evaluierung wird eine Liste von priorisierten Risiken unter Berücksichtigung der definierten Kriterien in Zusammenhang mit den Eintrittsszenarien, die ein derartiges Risiko verursachen, erlangt.

Als letzter wesentlicher Schritt ist das Ziel der Risiko-Behandlung die Definition, Auswahl und Anwendung von Maßnahmen zum Umgang mit den Risiken, beispielsweise zur Reduktion, Vermeidung, Veränderung, Transfer oder ggf. die Akzeptanz. Die jeweils zu wählenden Risiko-Behandlungsoptionen sollten gemäß /ISO18n03/ basierend auf den Ergebnissen des Risk Assessments gewählt werden, sowie basierend auf den erwarteten Kosten und der erwarteten Vorteile der Implementierung dieser Optionen. Daran anschließend muss das ggf. vorhandene Restrisiko bestimmt werden. Dies erfordert eine Aktualisierung oder erneute Iteration des Risk Assessments, einschließlich der erwarteten Auswirkung der vorgeschlagenen Risikobehandlung.

3.1.8 BSI-Standard 200-3 „Risikoanalyse auf der Basis von IT-Grundschutz“

Das Bundesamt für die Sicherheit in der Informationstechnik (BSI) entwickelt unter anderem Richtlinien und Standards zur Stärkung der Informationssicherheit. Darunter fällt beispielsweise der IT-Grundschutz als elementarer Schutz für Informationstechnik, der eine Vielzahl an Themengebieten abdeckt und beispielsweise den Anwendern helfen soll, sich gegen Cyberangriffe zu schützen. Ein Teil des Schutzes ist eine Risikoanalyse zum Umgang mit entsprechenden Risiken. Dies wird im BSI-Standard 200-3 /BSI17n02/ adressiert. Die Zielsetzung ist dabei, ein leicht anzuwendendes und anerkanntes Vorgehen in Bezug auf den angemessenen Umgang mit Informationssicherheitsrisiken zu illustrieren. Dieses Vorgehen beruht auf den im IT-Grundschutz-Kompendium beschriebenen elementaren Gefährdungen. Der gesamte Prozess zur Beurteilung und Behandlung von Risiken wird in /BSI17n02/ als Risikoanalyse bezeichnet. Der Begriff Risk Assessment ist mit der Risikoeinschätzung gleichzusetzen, die Teil der Risikoeinstufung (siehe unten) ist. Die Risikoanalyse nach /BSI17n02/ sieht im Wesentlichen 4 Schritte vor, die in Abb. 3.3 dargestellt sind und im Folgenden kurz zusammengefasst werden.

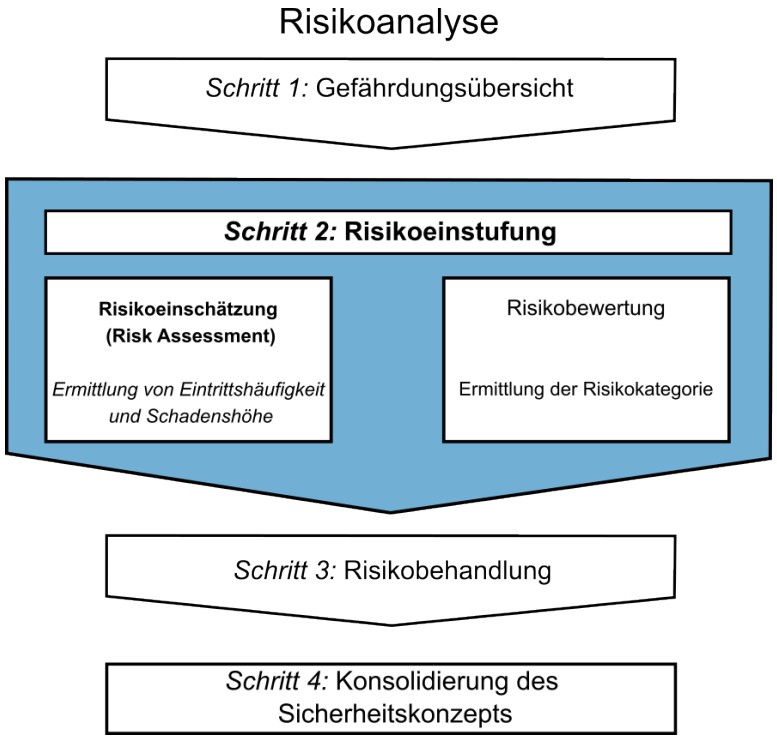

Abb. 3.3 Schritte der Risikoanalyse und Zusammenhang mit Risk Assessment laut BSI-Standard 200-3.

Der erste Schritt umfasst die Erstellung einer Gefährdungsübersicht. Nachdem die Vorarbeiten zur Risikoanalyse, die gemäß BSI-Standard 200-2 durchzuführen sind und beispielsweise eine Strukturanalyse und eine Schutzbedarfsfeststellung umfassen, abgeschlossen sind, liegt gemäß /BSI17n02/ eine Liste von Zielobjekten vor, die als Grundlage für die Erstellung einer Gefährdungsübersicht dient. Als Ausgangspunkt für eine Risikoanalyse erfolgt die Erstellung einer Übersicht über die Gefährdungen, die auf die betrachtenden Zielobjekte des Informationsverbundes einwirken. Für die Liste der Zielobjekte wird anschließend einer Risikoanalyse durchgeführt. Die Erstellung einer Gefährdungsübersicht besteht bei diesem Konzept aus zwei Stufen. Zunächst geht es um die Ermittlung und Identifizierung von relevanten elementaren Gefährdungen (diese sind im IT-Grundschutz definiert und umfassen beispielsweise Fehlfunktionen oder Ausfälle von Systemen oder Geräten). Dabei wird für jede elementare Gefährdung analysiert, ob diese direkt relevant ist und somit im Rahmen der Risikoanalyse weiter berücksichtigt wird oder nicht. Als Ergebnis ergibt sich eine Tabelle, in der jedem Zielobjekt eine Liste mit relevanten elementaren Gefährdungen zugeordnet ist und der Schutzbedarf jedes Zielobjektes vermerkt ist (im Rahmen der Schutzbedarfsfeststellung in den drei Grundwerten Vertraulichkeit, Integrität und Verfügbarkeit).

Die zweite Stufe umfasst die Ermittlung weiterer möglicher Gefährdungen, die über die elementaren Gefährdungen hinaus gehen und sich aus spezifischen Einsatzszenarios oder Anwendungsfällen ergeben.

Der zweite Schritt in /BSI17n02/ umfasst die Risikoeinstufung, die sich in eine Risikoeinschätzung und eine Risikobewertung aufteilt. Die Risikoeinschätzung ist mit dem Begriff des Risk Assessments gleichzusetzen. Nach der Identifizierung aller elementaren Gefährdungen erfolgt die Ermittlung des Risikos, dass mit einer Gefährdung einhergeht. Das ermittelte Risiko ist dabei von den Einflussgrößen Eintrittshäufigkeit und drohende Schadenshöhe abhängig. Grundsätzlich ist gemäß /BSI17n02/ eine qualitative oder quantitative Betrachtung von Risiken möglich, wobei angemerkt wird, dass eine quantitative Risikobetrachtung häufig sehr aufwendig ist und typischerweise ein umfangreiches statistische Datenmaterial voraussetzt. Eine qualitative Risikobetrachtung wird als häufig praktikabler für die Bewertung der Eintrittshäufigkeit und Schadenshöhe beschrieben. Der IT-Grundschutz nutzt dabei die Einteilungen in Kategorien wie *selten*, *mittel*, *häufig* und *sehr häufig* für die Eintrittshäufigkeit und *vernachlässigbar*, *begrenzt*, *beträchtlich* und *existenzbedrohend* für die Schadenshöhe. Mit den Definitionen der Schadenshöhe und der Eintrittshäufigkeit kann anschließend eine an die eigenen Bedürfnisse angepasste Risikomatrix zur Bewertung der Risiken erstellt werden. Mit Hilfe dieser Risikomatrix können die (qualitativen) Risikokategorien *gering*, *mittel*, *hoch* und *sehr hoch* festgelegt werden. Bei der Risikoeinstufung werden die geplanten oder bereits umgesetzten Sicherheitsmaßnahmen berücksichtigt und eine Übersicht über das Ausmaß der Risiken, die sich aus den Gefährdungen ergeben, erstellt.

Der dritte Schritt umfasst die Risikobehandlung. Eine Risikobehandlungsstrategie ist gemäß /BSI17n02/ von Organisation zu Organisation unterschiedlich und stark von der jeweiligen Risikobereitschaft einer Organisation abhängig, sodass unterschiedliche Risikoakzeptanzkriterien möglich sind. In /BSI17n02/ wird dabei angenommen, dass „geringe“ Risiken grundsätzlich akzeptiert werden, jedoch „mittlere“, „hohe“ und „sehr hohe“ nur in Ausnahmefällen akzeptiert werden. Die Gefährdungen werden in der Praxis in der Regel in den Risikostufen „mittel“, „hoch“ oder „sehr hoch“ eingestuft. Für den Umgang mit den verbleibenden Risiken müssen geeignete Risikobehandlungsoptionen ausgewählt werden. Risiken können gemäß /BSI17n02/ akzeptiert, vermieden, reduziert oder transferiert werden. Aufbauend auf den Risikobehandlungsoptionen Vermeidung, Reduktion und Transfer muss eine Organisation Risikoakzeptanzkriterien festlegen und die Risikobehandlung darauf abbilden.

Für jede Gefährdung mit der Risikokategorie „mittel“, „hoch“ oder „sehr hoch“ muss entschieden werden, ob es sinnvoll ist, dass Risiko zu vermeiden, zu reduzieren/modifizieren oder zu transferieren/aufzuteilen oder ob aufgrund der Faktenlage das Risiko akzeptiert werden kann. Die Schritte der Risikoeinstufung und Risikobehandlung werden iterativ so lange durchlaufen, bis die Risikoakzeptanzkriterien der Organisation erreicht sind und das verbleibende Risiko („Restrisiko“) im Einklang mit den Zielen und Vorgaben der Organisation steht. Als weiterer Aspekt der Behandlung von Risiken gilt es im Rahmen der Risikobeobachtung ergänzende Sicherheitsmaßnahmen für Gefährdungen zu erarbeiten, die momentan akzeptabel sind, aber in Zukunft Handlungsbedarf erfordern könnten. Dadurch können die im Vorfeld vorbereiteten Sicherheitsmaßnahmen umgesetzt werden, sobald die Risiken inakzeptabel werden. Dafür werden die Risiken fortlaufend beobachtet und die Sicherheitsmaßnahmen überprüft und gegebenenfalls aktualisiert, sowie die Risikoeinstufung angepasst.

Der letzte Schritt umfasst die Konsolidierung des Sicherheitskonzepts. Wenn ergänzende Maßnahmen zu den bereits im Sicherheitskonzept beschriebenen Sicherheitsmaßnahmen hinzugefügt werden müssen, ist eine anschließende Konsolidierung des Sicherheitskonzepts erforderlich. Dies bedeutet, dass die Sicherheitsmaßnahmen für jedes Zielobjekt überprüft werden müssen. Dabei ist unter anderem zu klären, ob die Sicherheitsmaßnahmen zur Abwehr von Gefährdungen geeignet sind, wie sie mit zusammenwirken, wie benutzerfreundlich sie sind und ob sie angemessen sind.

3.1.9 ISO/SAE 21434 „Road vehicles – Cybersecurity engineering”

Der Standard /ISO21n01/ befasst sich mit der Cybersicherheitsperspektive bei der Entwicklung elektrischer und elektronischer Systeme in Straßenfahrzeugen. Er behandelt die Anforderungen für das Cyber-Risikomanagement in Bezug auf das Konzept, die Produktentwicklung, die Produktion, den Betrieb, die Instandhaltung und die Außerbetriebnahme der elektrischen und elektronischen Systeme von Fahrzeugen, einschließlich derer Komponenten und Schnittstellen. Im Rahmendes Vorhabens relevante Inhalte und Aspekte finden sich insbesondere im Abschnitt zum Thema „Threat analysis and risk assessment (TARA) methods“. Diese Inhalte werden im Folgenden kurz zusammengefasst.

Im Abschnitt zur Bedrohungsanalyse und Risikobewertung von /ISO21n01/ geht es um die Beschreibung von Methoden zur Bestimmung des Umfangs, in dem ein Verkehrsteilnehmer aus dessen Sichtweise durch ein Bedrohungsszenario beeinflusst werden kann.

Die definierten Methoden sind dabei generische Bausteine/Module, die an jedem Punkt des Lebenszyklus eines Items oder einer Komponente systematisch aufgerufen werden können. Als Ziele der Bedrohungsanalyse und Risikobewertung werden die folgenden Punkte genannt, die in Abb. 3.5 veranschaulicht sind:

- Identifizierung der Assets und deren IT-Sicherheitseigenschaften, sowie deren Schadensszenarien
- Identifizierung der Bedrohungsszenarien
- Bestimmung der Bewertung der Auswirkungen der Schadensszenarien
- Identifizierung der Angriffspfade die ein Bedrohungsszenario ermöglichen
- Bestimmung der Durchführbarkeit eines Angriffspfads
- Bestimmung des Risikowertes eines Bedrohungsszenarios und
- Auswahl von angemessenen Risikobehandlungsoptionen für Bedrohungsszenarien;

Diese einzelnen Schritte der TARA werden im Folgenden kurz zusammengefasst.

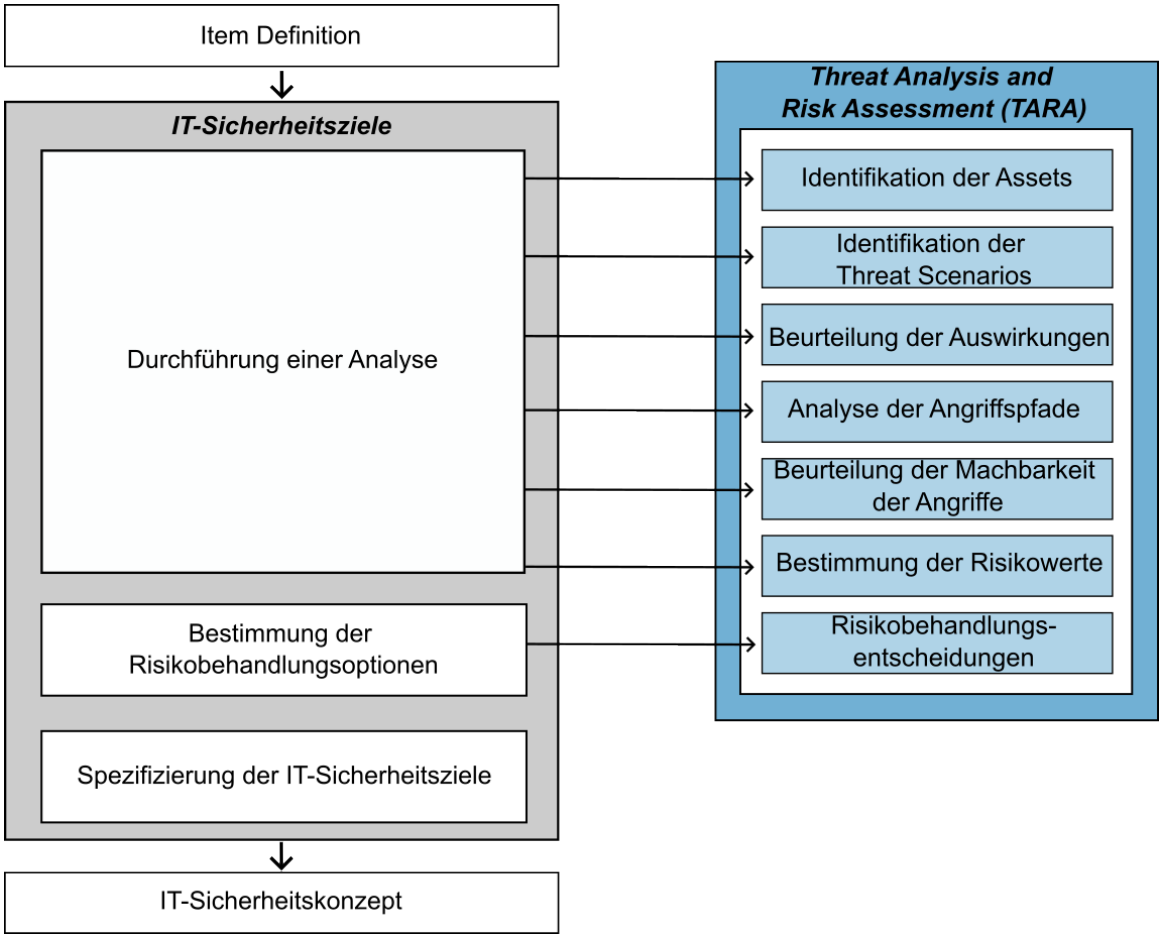

Abb. 3.4 Einordnung der Threat Analysis and Risk Assessment (TARA) in die IT-Sicherheitsziele mit den einzelnen Schritten laut ISO/SAE 21434

In Bezug auf die Identifizierung der Assets sollen gemäß /ISO21n01/ Schadensszenarien sowie die Assets relevant für die Cybersicherheit, deren Kompromittierung zu einem Schadensszenario führen könnte, identifiziert werden. Das Arbeitsergebnis sind dann identifizierte Schadensszenarien und die zugehörigen Assets. Dazu soll im Rahmen der Identifizierung der Bedrohungsszenarien relevante Szenarien, welche die jeweiligen Ziele/Assets, die kompromittierten Eigenschaften der Cybersicherheit der Assets und die zugrundeliegende Problematik in Bezug auf eine solche Kompromittierung berücksichtigen.

Im nächsten Schritt geht es in /ISO21n01/ um die Beurteilung von potenziellen Auswirkungen. Die Beurteilung basiert auf den vorigen Schritten, sodass die identifizierten Schadensszenarien hinsichtlich potenzieller negativer Auswirkungen in Bezug auf Sicherheit, Finanzen, Betrieb und Datenschutz (Auswirkungskategorien) für die Verkehrsnutzer bewertet werden sollen.

Dabei sollte die Bewertung der Auswirkung eines Schadensszenarios hinsichtlich der oben genannten Kategorien erfolgen und den Stufen „sehr schwer“, „erheblich“, „mäßig“ und „vernachlässigbar“ zugeordnet werden. Als Arbeitsergebnis ergibt sich in diesem Schritt die Bewertung der Auswirkungen mit den zugehörigen Auswirkungskategorien.

Im Rahmen der Analyse möglicher Angriffspfade sind unter anderem Informationen zu IT-Sicherheitsvorfällen und zugehörigen Schwachstellen, während der Entwicklung gefundene Schwachstellen, die Architektur, bereits identifizierte Angriffspfade und weitere Schwachstellen-Analysen relevant. Die Bedrohungsszenarien sollten dabei zur Identifizierung von Angriffspfaden analysiert werden, wobei gemäß /ISO21n01/ entweder ein Top-down-Ansatz, bei dem Angriffspfade ausgehend von Bedrohungsszenarien hinsichtlich der Realisierung betrachtet werden, oder ein Bottom-up-Ansatz, bei dem ausgehend von den Schwachstellen der eigenen Systeme mögliche Angriffspfade betrachtet werden, verwendet werden kann. Ein Angriffspfad sollte entsprechend dem Bedrohungsszenario zugeordnet werden, welches durch den Angriffspfad realisierbar ist. Als Arbeitsergebnis erhält man somit die Angriffspfade.

Aufbauend auf diesen Pfaden geht es im nächsten Schritt von /ISO21n01/ um die Bewertung der Durchführbarkeit eines entsprechenden Angriffs. Dabei sollte für jeden Angriffspfad die Bewertung der Durchführbarkeit des Angriffs anhand der Einteilung von „hoch“ (der Angriffspfad kann mit geringem Aufwand ausgenutzt werden) über weitere Zwischenstufen bis „sehr gering“ (der Angriffspfad kann mit sehr hohem Aufwand ausgenutzt werden) bewertet werden. Die in /ISO21n01/ dazu genannte Methodik umfasst dabei einen Ansatz basierend auf dem Angriffspotential (berücksichtigt unter anderem zeitliche Faktoren, fachliche Kompetenz, Wissen über das Asset oder die Komponente, verfügbares Zeitfenster und Ausrüstung) einen Ansatz basierend auf dem allgemeinen Schwachstellen-Bewertungssystems (engl.: Common Vulnerability Scoring System, CVSS, unter anderem basierend auf Angriffsvektoren, Komplexität des Angriffs, erforderliche Berechtigungen und Benutzerinteraktion) und einen Ansatz basierend auf den Angriffsvektoren. Aufbauend auf diesen Überlegungen folgt in /ISO21n01/ die Bestimmung des Risikowertes. Für jedes Bedrohungsszenario soll dabei ein Risikowert anhand der Auswirkung eines Schadensszenarios und der Machbarkeit des Angriffs des zugehörigen Angriffspfades bestimmt werden. Der Risikowert eines Bedrohungsszenarios sollte einen Wert zwischen 1 und 5 haben, wobei 1 ein minimales Risiko repräsentiert.

Als letzter Schritt wird in /ISO21n01/ im Rahmen des betrachteten Prozesses das Thema Risikobehandlung adressiert.

Dabei sollten die in den vorigen Schritten erlangten Informationen berücksichtigt werden. Für jedes Bedrohungsszenario sollte unter Beachtung des Risikowertes im Rahmen der Risikobehandlungsoptionen bestimmt werden, ob das entsprechende Risiko zu vermeiden ist, verringert werden muss, geteilt werden muss (beispielsweise durch den Abschluss einer Versicherung), oder ob das Risiko beibehalten wird. Mit der abschließenden Entscheidung zur Risikobehandlung endet dieser Abschnitt zur Bedrohungsanalyse und zum Risk Assessment in /ISO21n01/.

3.1.10 ISO/IEC 18045 „Information security, cybersecurity and privacy protection – Evaluation criteria for IT security – Methodology for IT security evaluation"

Die Norm ISO/IEC 18045 „Information security, cybersecurity and privacy protection – Evaluation criteria for IT security – Methodology for IT security evaluation" /ISO22n01/ behandelt Vorgaben, die von einem Gutachter zur Evaluierung nach der ISO/IEC 15408 Serie durchgeführt werden sollten. Im Wesentlichen legt die Norm ISO/IEC 15408 „Information security, cybersecurity and privacy protection - Evaluation criteria for IT security" allgemeine Konzepte und Grundsätze zur Evaluierung der IT-Sicherheit fest und die Norm ISO/IEC 18045 beschreibt die Vorgehensweise und Methodik, wie eine Bewertung tatsächlich durchgeführt wird.

In Bezug auf das Vorhaben sind insbesondere die Textinhalte zum Thema Schwachstellen-Assessment relevant. Das Ziel des Assessments ist dabei, die Ausnutzbarkeit von Fehlern oder Schwächen als Evaluierungsgegenstand in der Betriebsumgebung zu bestimmen. Dazu sollen unter anderem öffentlich verfügbare Informationen sowie ggf. Penetrationstests durch den Evaluierenden durchgeführt werden. In /ISO22n01/–wird die Schwachstellenanalyse je nach angenommenem Angriffspotenzial des Angreifers (Basic, Enhanced-Basic, Moderat, High) unterschieden, woraufhin unterschiedliche Vorgaben für die Evaluierung gemacht werden.

3.2 Länderspezifische Vorgehensweise

Das US-amerikanische National Institute of Standards and Technology (NIST) ist eine dem US-Handelsministerium unterstellte Großforschungseinrichtung. Das NIST forscht in und entwickelt Standards zu verschiedensten technischen Themenbereichen wie Messtechnik, Kommunikationstechnik, Ingenieurwissenschaften, Informationstechnik.

Im Februar 2014 veröffentlichte das NIST das NIST Cybersecurity Framework /NIS24n01/, welches verschiedene Richtlinien für die Identifikation und die Bewertung sowie das Management und die Reduktion von Risiken im Bereich der Cybersicherheit bereitstellt. Hierbei setzt das Framework bei übergeordneten Funktionen an (siehe Abb. 3.5). Diese reichen von der

- Festlegung, Kommunikation und Überwachung der Cybersicherheits-Strategie („govern“), über
- Verständnis der Cybersicherheits-Risiken („identify“) bis hin zum
- Ergreifen von Maßnahmen zur Verhinderung von Cyberangriffen („protect“), zur
- Feststellung von Kompromittierungen und Cyberangriffssituationen („detect“), zum
- Ergreifen von Maßnahmen hinsichtlich eines festgestellten Cyberangriffs („respond“) sowie zur
- Wiederherstellung der Cybersicherheit von Assets und Prozessen, die von einem festgestellten Cyberangriff betroffen waren („recover“)

Abb. 3.5 Funktionen des NIST Cybersecurity Frameworks /NIS24n01/

Das Framework bezieht sich für das Risk Management auf drei Ebenen: Die Organisationsebene, die Prozessebene und die Systemebene, die sich hinsichtlich des Risk Managements sowohl vom Detaillierungsgrad der Betrachtung als auch von der Granularität der Perspektive her unterscheiden (siehe Abb. 3.6).

Sowohl durch die Fokussierung auf Funktionen, für die einzelne Aufgaben definiert werden, als auch durch die Struktur unterschiedlicher Ebenen unterstützt das Framework eine systematische Vorgehensweise bei der Risikobetrachtung.

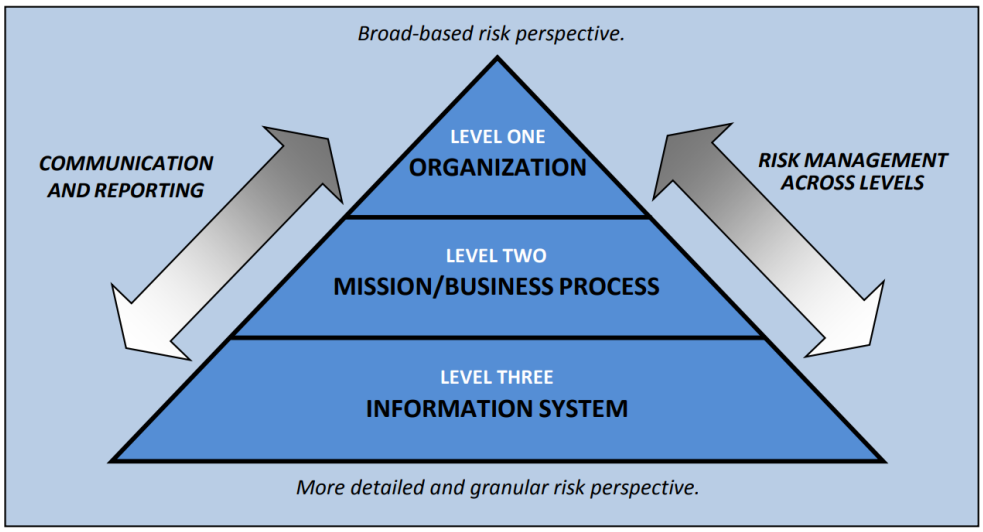

Abb. 3.6 Ansatz für ein organisationsweites Risk Management gemäß /NIS24n01/

Dieses 2014 entwickelte und 2024 überarbeitete, übergeordnete Framework wird inzwischen im Zusammenspiel mit den bereits länger etablierten, spezifischen Standards für Cybersecurity Risk Management und Assessment der NIST angewendet. Hierbei sind insbesondere die Standards

- SP 800-37, Risk Management Framework for Information Systems and Organizations /NIS18n01/,
- SP 800-30, Guide for Conducting Risk Assessments /NIS12n01/

des allgemeinen NIST Risk Management Frameworks (RMF) sowie die Standards

- SP 800-39, Managing Information Security Risk /NIS11n01/
- SP 800-53, Security and Privacy Controls for Information Systems and Organizations /NIS20r01/

wesentlich. Die NIST stellt in diesen Veröffentlichungen insgesamt eine systematische Herangehensweise für Risk Management und Risk Assessment vor, wobei das übergeordnete Framework sehr breit angelegt und auf den Prozess des Risk Managements ausgerichtet ist, hierbei aber nur einen geringen Detailierungsgrad aufweist. Die NIST SP 800-30 bezieht sich im Wesentlichen auf Risk Assessment, hat also eine hinsichtlich der Betrachtungsbreite deutlich spezialisiertere Ausrichtung, allerdings mit

deutlich ausgeprägterer Betrachtungstiefe. Die NIST SP 800-53 setzt darunter an und weist eine eng gefasste Betrachtung mit für diesen Betrachtungsbereich höherem Detaillierungsgrad auf. Ähnlich lassen sich die weiteren Standards der NIST, die mit Risk Management oder Risk Assessment in Zusammenhang stehen, einordnen.

In den folgenden Abschnitten werden die für das Vorhaben relevanten Inhalte des zentralen Standards 800-30 sowie beispielhaft des Standards 800-53 kurz vorgestellt.

3.2.1 NIST 800-30 „Information Security - Guide for Conducting Risk Assessments“

Der US-amerikanische Standard NIST 800-30 /NIS12n01/ beschäftigt sich fast ausschließlich mit dem Thema Risk Assessment und gilt als Leitfaden zur Durchführung des Risk Assessments für die Vereinigten Staaten. Die Entwicklung des Standards wurde u. a. unterstützt von zivilen Einrichtungen, sowie Verteidigungs- und Nachrichtendiensten der USA. Der Standard wird inzwischen auch international breit angewendet. Der Schwerpunkt des Standards liegt auf dem Risk Assessment als wesentlicher Bestandteil eines zielführenden Risiko Managements. Er beschreibt ein strukturiertes Vorgehen, um Risiken zu identifizieren, zu analysieren und nach Prioritäten zu ordnen, mit dem Ziel, Entscheidungsträgern informierte Entscheidungen hinsichtlich der Reaktion auf die verschiedenen Risiken zu ermöglichen. Dabei wird zunächst das grundlegende Konzept eines Risk Management Prozesses beschrieben und die Einordnung des Risk Assessments als zentraler Bestandteil dieses Prozesses erläutert. Abb. 3.7 gibt den in NIST SP 800-30 beschriebenen Risk Management Prozess wieder. Zentraler Punkt ist hierbei der erste Schritt des Risk Managements (Risikokontextualisierung), in dem eine Beschreibung des Risikokontextes erfolgt, d. h. eine Festlegung des Rahmens, innerhalb dem die risikobasierten Entscheidungen getroffen werden. Zur Kontextualisierung des Risikos gehören u. a. die Risikoannahmen über die Bedrohungen, Schwachstellen, Folgen/Auswirkungen und die Risikotoleranz (z. B. akzeptable Risiken, Risikotypen und akzeptable Risikounsicherheit). Im zweiten Schritt (Risk Assessment) werden die Bedrohungen für die Organisationen (d. h. für den Betrieb, die Assets oder Personen) oder Bedrohungen, die von Organisationen auf andere Organisationen ausgehen, ermittelt. Zusätzlich erfolgt eine Ermittlung von Schwachstellen innerhalb und außerhalb von Organisationen sowie des Schadens, der entstehen kann, wenn das Bedrohungspotenzial genutzt wird. Gegebenenfalls kann auch die Eintrittswahrscheinlichkeit für den Schadensfall in diesem Schritt eine Rolle spielen. Das Ziel des Risk Assessments sind evaluierte Risiken.

Im dritten Schritt (Umgang mit den Risiken) wird der Umgang mit den im Risk Assessment ermittelten Risiken bestimmt, um ein einheitliches, organisationsweites Vorgehen zu gewährleisten. Hierzu gehören die Ermittlung und Evaluierung von Handlungsmöglichkeiten in Übereinstimmung mit der organisatorischen Risikotoleranz, sowie die Umsetzung von Maßnahmen. Der vierte und letzte Schritt (Risikobeobachtung) beinhaltet die fortlaufende Kontrolle der Wirksamkeit der Risikobehandlung. Das Ziel der Risikobeobachtung ist die Überprüfung, ob die Maßnahmen zum Umgang mit den Risiken umgesetzt und die Anforderungen an die Informationssicherheit erfüllt werden, die sich aus den Aufgaben der Organisation, den Gesetzen, Richtlinien, Vorschriften, Grundsätzen, Standards und Leitlinien ergeben.

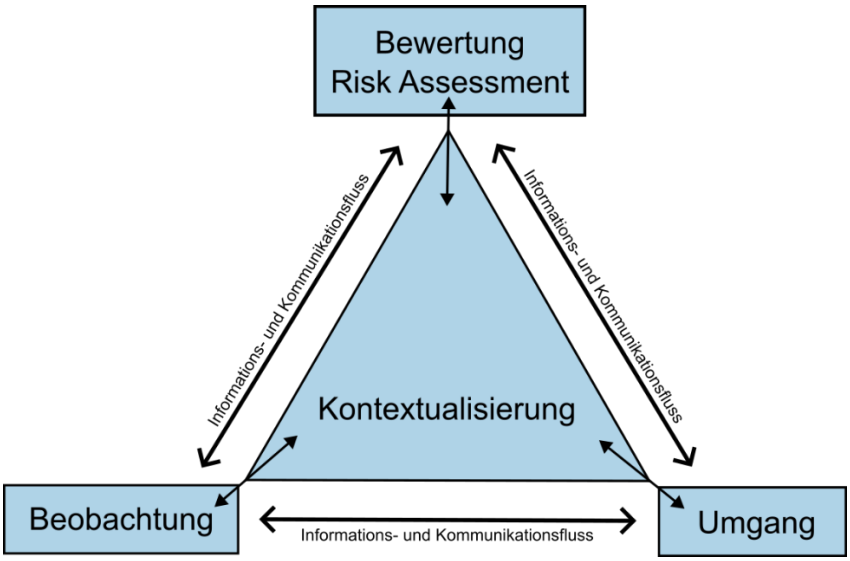

Abb. 3.7 Zusammenhang der vier Bestandteile des Risikomanagement Prozesses laut NIST 800 30

Der Schwerpunkt der NIST SP 800-30 liegt auf dem Risk Assessment als Teil des Risikomanagements und beschreibt detailliert nicht nur die Durchführung eines Risk Assessments, sondern auch die Schritte der Vorbereitung des Risk Assessment, der Kommunikation der Ergebnisse des Risk Assessments an die Entscheidungsträger sowie die Erhaltung und Fortführung des Risk Assessments (siehe Abb. 3.8). Insbesondere der letzte Punkt unterstreicht, dass die Durchführung eines Risk Assessments keine einmalige Tätigkeit ist, sondern vielmehr von Organisationen kontinuierlich eingesetzt werden muss. So wird Risk Assessment während des gesamten Lebenszyklus eines IT-Systems und über alle Stufen der Risikomanagement-Hierarchien angewendet.

Auch sind die Gültigkeit und Nützlichkeit jedes Risk Assessments zeitlich begrenzt, da sich Unternehmensfunktionen und -prozesse, sowie Informationssysteme, Bedrohungen und Betriebsbedingungen im Laufe der Zeit ändern.

NIST SP 800-30 stellt den Prozess des Risk Assessment vor allem als Instrument in den Händen der Organisation dar, die ihn einsetzt: Zum einen, um die potenziellen nachteiligen Auswirkungen aufzuzeigen, die sich aus den bestehenden Risiken für den Betrieb und die materiellen oder immateriellen Assets der Organisation, sowie für Individuen, andere Organisationen, oder die wirtschaftlichen und nationalen Sicherheitsinteressen der USA, ergeben können, und zum anderen, um bei einer großen Bandbreite von risikobasierten Entscheidungen zu assistieren und Tätigkeiten von Entscheidungsträgern über alle Ebenen der Risikomanagement-Hierarchie zu unterstützen.

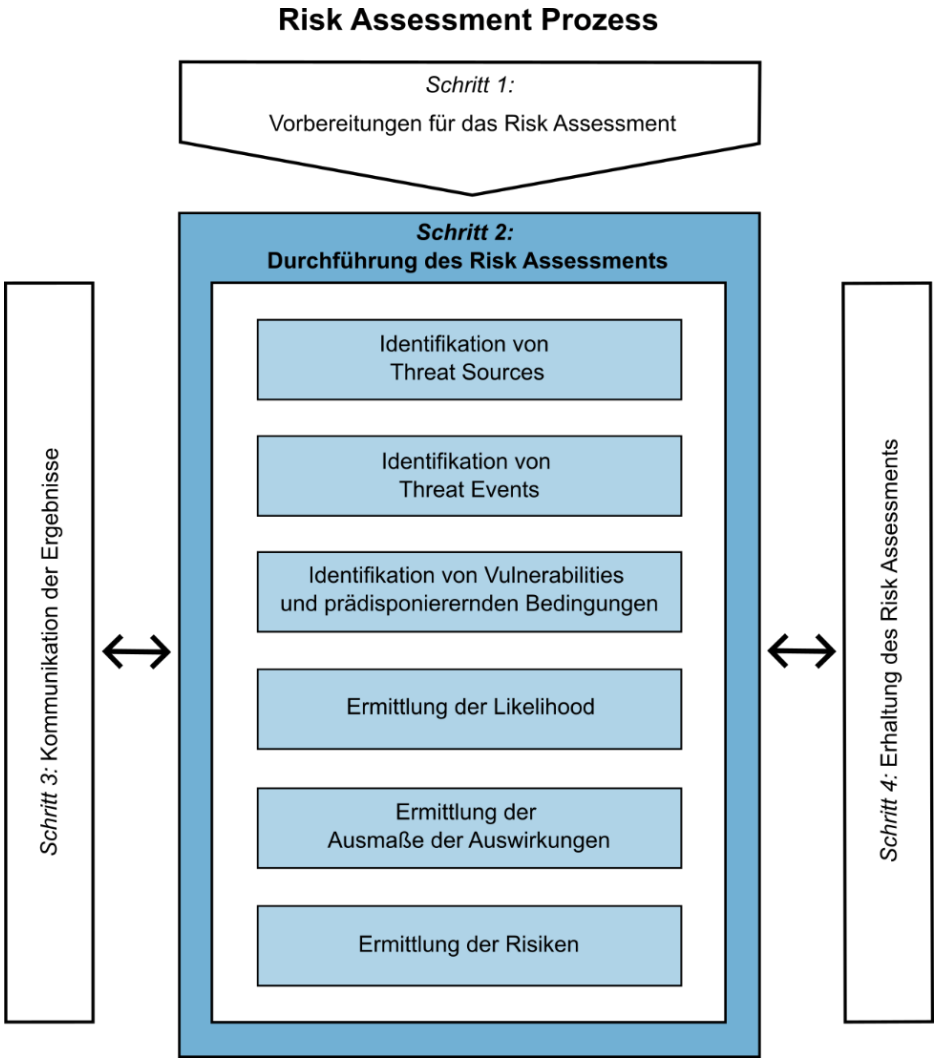

Abb. 3.8 Schritte des Risk Assessment Prozesses und Aktivitäten der Durchführung (Schritt 2) gemäß NIST 800-30

Den Rahmen für das Risk Assessment sollten laut NIST SP 800-30 die im Vorbereitungsschritt festgelegten spezifischen Definitionen und Richtlinien, sowie die Analyseansätze des Risk Assesments und die Gewährleistung einer angemessene Abdeckung der Bedrohungslage bilden. Ein weiteres Ziel der Vorbereitungsschrittes für das Risk Assessments besteht darin, eine Verknüpfung zum Schritt der Risikokontextualisierung des zuvor beschriebenen Risk Management Prozesses herzustellen und diesen Kontext durch die Identifizierung von Randbedingungen wie Zweck und Umfang des Risk Assessments, Annahmen und Einschränkungen für dessen Durchführung sowie nutzbare Informationsquellen und anwendbare Risikomodelle und Analyseansätze weiter zu konkretisieren.

Ziel der anschließenden Durchführung des Risk Assessments ist die Erstellung einer Liste der Risiken für die Informationssicherheit, die dann anhand von vordefinierten Risikostufen priorisiert und zur Entscheidungsfindung für den Umgang mit den Risiken verwendet werden kann. Für die Erreichung dieses Ziels werden Bedrohungen und Schwachstellen identifiziert und analysiert, die potenziellen Auswirkungen sowie ggf. die Eintrittswahrscheinlichkeiten ermittelt, sowie die Unsicherheiten bestimmt, die mit dem Risk Assessment Prozess in Verbindung stehen. Die Ergebnisse des Risk Assessments werden anschließend so kommuniziert, dass die Entscheidungsträger im gesamten Unternehmen über die entsprechenden risikobezogenen Informationen verfügen, anhand derer informierte Entscheidungen getroffen werden können. Der letzte, aber sehr wesentliche Schritt besteht in der Erhaltung und Fortführung des Risk Assessments. Hierbei ist das Ziel, das spezifische Wissen über die identifizierten Risiken, die damit einhergehenden potenziellen Auswirkungen und den Umgang mit ihnen aktuell zu halten. Um die fortlaufende Überprüfung der Entscheidungen im Rahmen des übergeordneten Risk Managements zu unterstützen, wird das Risk Assessment permanent aufrechterhalten. Hierzu gehört vor allem die Berücksichtigung von Änderungen, die beispielsweise in Bezug auf Bedrohungen, IT-Systeme, Prozesse oder Prozeduren bekannt werden oder geplant bzw. vorgenommen werden. Ein weiterer, in engem Zusammenhang mit dem Risk Assessment stehende Aspekt ist die Risikoüberwachung. Hierbei steht die Wirksamkeit von Sicherungsmaßnahmen – technische Sicherungsmaßnahmen genauso wie personelle und administrative – in Bezug auf die Risiken im Vordergrund.

Über diese am Risk Assessment Prozess orientierten Anforderungen mit dem Schwerpunkt auf konkrete Handlungsschritte hinaus beschäftigt sich die NIST SP 800-30 auch mit Risk Assessment Methodik und mit dem Aspekt wie genau diese Handlungsschritte ausgeführt werden sollten. Die NIST setzt hierbei grundsätzlich bei der Erstellung und Beschreibung von Methodiken für die Durchführung eines Risk Assessments an. So beinhaltet eine Risk Assessment Methode gemäß NIST SP 800-30 typischerweise die folgenden Schritte:

- einen Risk Assessment Prozess (siehe oben),
- ein Risikomodell, welches die Schlüsselbegriffe und bewertbaren Risikofaktoren, sowie die Zusammenhänge zwischen diesen Faktoren, definiert,
- eine Herangehensweise bei der Bewertung von Eintrittswahrscheinlichkeiten (beispielsweise qualitativ, quantitativ und semi-quantitativ)
- einen grundlegenden Analyseansatz (beispielsweise bedrohungs-, konsequenz oder schwachstellen-basiert).

Welche Methode bzw. Methoden für die Durchführung eines Risk Assessments anzuwenden sind, wird im Rahmen der Risikomanagement-Strategie von der Organisation festgelegt.

Bei der Bewertung von Eintrittswahrscheinlichkeiten gibt es zwei grundlegend verschiedene Ansätze: quantitative und qualitative Bewertungen. Darüber hinaus gibt es noch die Mischform der semi-quantitativen Bewertung. Grundsätzlich beruhen quantitative Bewertungen auf numerischen Ansätzen und ermitteln auf Basis von Rechenregeln Zahlenwerte, was bedeutet, dass die zu berücksichtigenden Risikofaktoren zunächst ebenfalls beziffert werden müssen. Im Gegensatz dazu stehen qualitative Bewertungen, die auf nicht-nummerischen Kategorien oder Einstufungen (beispielsweise sehr niedrig, niedrig, mittel, hoch, sehr hoch) basieren. Bei semi-quantitativen Bewertungen werden typischerweise Kategorien, Skalen oder repräsentative Zahlen angewendet. Hierbei weist die NIST darauf hin, dass die jeweiligen Ergebnisse unabhängig von der Art der Bewertung nur temporäre Gültigkeit besitzen.

Die Analyseansätze unterscheiden sich hinsichtlich der Ausrichtung oder des Ausgangspunktes des Risk Assessments. Die NIST SP 800-30 geht dabei auf den Bedrohungs-basierten (threat-oriented), Konsequenz-basierten (impact-oriented) oder Schwachstellen-basierten (vulnerability-oriented) Ansatz ein.

Insgesamt betrachtet die NIST Risk Assessments vornehmlich in Bezug auf Informationssysteme. Hierbei wird deutlich gemacht, dass das Risk Assessment nicht nur punktuell innerhalb des Lebenszyklus eines Informationssystems eine Rolle spielt, sondern dass Risikobetrachtungen über den gesamten Lebenszyklus des Systems hinweg wesentlich sind.

3.2.2 NIST 800-53 „Security and Privacy Controls for Information Systems and Organizations“

Der Fokus der NIST SP 800-53 /NIS20r01/ liegt auf Sicherungsmaßnahmen für Systeme und die Organisationen allgemein. Dieser Standard setzt also im Wesentlichen beim Aspekt der Definition, Planung und Umsetzung von Sicherungsmaßnahmen zur Risikobehandlung an. Diese sowie weitere NIST Publikationen sind erstellt worden, um Organisationen bei der Identifizierung von geeigneten Sicherungsmaßnahmen zu unterstützen. Im Fall der NIST SP 800-53 zählen hierzu insbesondere auch Datenschutzregelungen.

Das Dokument stellt einen umfassenden Katalog von flexiblen und individuell gestaltbaren Sicherungsmaßnahmen zur Verfügung. Dabei werden zahlreiche Bereiche behandelt, darunter beispielsweise Zugangskontrollen, Awareness und Training, Instandhaltung und personenbezogene Daten. Darüber hinaus ist der Standard inhaltlich eng mit den Risk Assessment und Risk Management Prozessen verknüpft. So geht er neben Richtlinien und Verfahren unter anderem auf die Aktualisierung des Risk Assessments, das Scannen nach Schwachstellen, die oben bereits genannte Risikobehandlung sowie auf die Betrachtung von Fragen des Datenschutzes auch auf Kritikalitätsanalysen in Bezug auf Risiken sowie auf Threat Hunting ein. Über Sicherungsmaßnahmen hinaus soll die NIST SP 800-53 auch zur Verbesserung von Kommunikation zwischen und innerhalb von Organisationen beitragen, indem sie ein Glossar zur Verfügung stellt, welches die Diskussion von Konzepten für Sicherheit, Datenschutz, und Risikomanagement unterstützt.

Die NIST SP 800-53 stellt Risk Assessment im Kontext von Bedrohungen, Schwachstellen, Wahrscheinlichkeiten und Auswirkungen dar, betont dabei aber die wesentlichen Einflüsse von Akteuren außerhalb der Organisation. Hierbei sind insbesondere Akteure in der Lieferkette gemeint wie beispielsweise Auftragnehmer, die ein System der Organisation bedienen und Individuen, die Zugriff auf die Systeme der Organisation haben, sowie die Serviceanbieter und ausgelagerte Einheiten.

Analog zu NIST 800-30 weist auch dieser Standard darauf hin, dass Risk Assessment in allen Managementebenen und während jedes Schritts im Lebenszyklus eines Systems durchführbar ist. Auch verknüpft er die Durchführung von Risk Assessments mit verschiedenen Schritten des Risk Management Rahmens, einschließlich der Vorbereitung, Kategorisierung, Auswahl, Implementierung, Autorisierungen und der Überwachung von Sicherungsmaßnahmen. Des Weiteren geht die NIST SP 800-53 kurz auf die Aspekte Verwendung von Informationen aus zahlreichen Quellen im Rahmen der Risikoanalyse, dynamisches Bewusstsein für Bedrohungen und prädiktive Analytik, d. h. die Vorhersage zukünftiger Ereignisse auf Basis historischer Daten, ein.

4 Vergleichende Betrachtung

Die bisher dargestellten Arbeitsergebnisse unterstreichen deutlich Gemeinsamkeiten und Unterschiede in den verschiedenen betrachteten Vorgehensweisen zum Risk Assessment. In den folgenden Abschnitten werden zunächst unterschiedliche Ansätze für das Risk Assessment diskutiert (siehe Abschnitt 3.1). Dabei wird die Blickrichtung der einzelnen Ansätze (siehe Abschnitt 3.2) diskutiert. Zudem werden Unterschiede bei der Herangehensweise an den Umgang mit Wahrscheinlichkeiten im Rahmen des Risk Assessments (siehe Abschnitt 3.2) betrachtet.

4.1 Risk Assessment: Unterschiedliche Ansätze

Für die Durchführung eines Risk Assessments gibt es grundsätzlich verschiedene Ansätze, je nachdem, welcher Ausgangspunkt für die Ermittlung des Risikos, die Risikoanalyse und die Evaluation des Risikos gewählt wird:

- Bedrohungs-basierter Ansatz
- System-basierter Ansatz
- Schwachstellen-basierter Ansatz
- Konsequenz-basierter Ansatz

Die grundsätzlichen Unterschiede zwischen den einzelnen Vorgehensweisen bei der Durchführung eines Risk Assessments lassen sich einerseits in Bezug auf die Bewertung der Risiken und der zugehörigen relevanten Faktoren und andererseits anhand der jeweiligen Blickrichtung diskutieren. Im Folgenden werden diese Aspekte kurz beschrieben.

Bedrohungs-basierter Ansatz

Bei einem Bedrohungs-basierten Ansatz des Risk Assessments stehen potenzielle Bedrohungen im Mittelpunkt der Betrachtungen. Der Begriff Bedrohung umfasst dabei jeglichen Umstand oder Ereignis, durch den oder das potenziell eine unerwünschte Konsequenz eintreten kann. Bedrohungen müssen hierbei nicht zwangsläufig mit maliziösen Angreiferhandlungen oder Intentionen in Zusammenhang stehen. Vielmehr können sie auch unabsichtliche Handlungen sowie externe Bedingungen wie beispielsweise Naturereignisse beinhalten. Der Bedrohungs-basierte Ansatz setzt bei den Bedrohungen an,

die durch konkrete Bedrohungsereignisse in Verbindung mit einer oder mehrerer Bedrohungsquellen beschrieben werden. Daraus werden Bedrohungsszenarien entwickelt, was zu einer Identifikation von potenziellen Angriffsvektoren und Schwachstellen und somit zur Identifikation von konkreten Angriffsszenarien führt, woraufhin sich der Schwerpunkt auf die möglichen Auswirkungen verlagert.

Schwachstellen-basierter Ansatz

Im Rahmen eines Schwachstellen-basierten Ansatzes des Risk-Assessments stehen Schwachstellen im Mittelpunkt der Betrachtungen. In diesem Zusammenhang bezeichnet der Begriff Schwachstelle eine Anfälligkeit oder Verwundbarkeit in einem IT-System, (sicherheits- und/oder sicherungsrelevanten) Abläufen oder Sicherheits- und Sicherungsmaßnahmen, die von einem Angreifer ausgenutzt werden kann. Schwachstellen sind beispielsweise insbesondere im Zusammenhang mit digitalen Systemen (Systeme zur Informationsverarbeitung, Systeme zur Automation, Leittechniksysteme etc.) relevant und ermöglichen potenziellen Angreifern durch ihre Ausnutzung verschiedene Angriffsschritte. Schwachstellen in organisatorischen Abläufen und Prozessen sowie Schwachstellen mit Bezug zum Faktor Mensch müssen ebenfalls berücksichtigt werden. Darüber hinaus stellen auch Schwachstellen in Zusammenhang mit nicht oder ungenügend umgesetzten Sicherungsmaßnahmen oder Sicherungsmaßnahmen mit verbleibenden Schwachpunkten mögliche Angriffspunkte dar. Der Schwachstellen-basierte Ansatz setzt somit im Wesentlichen bei Angriffsvektoren im Zusammenhang mit Schwachstellen an, die von Angreifern ausgenutzt und zur Herbeiführung von Bedrohungsereignissen eingesetzt werden können. Bei einer allgemeinen Anwendung des schwachstellen-basierten Ansatzes werden neben Bedrohungen, die mit absichtlichen Angreiferhandlungen in Zusammenhang stehen, auch Bedrohungen wie Naturereignisse mit betrachtet.

System-basierter Ansatz

Der System-basierte Ansatzes des Risk-Assessments setzt bei den eingesetzten Systemen und sich daraus ergebenden Risiken an. Dabei werden alle digitalen Systeme, (Systeme zur Informationsverarbeitung, Systeme zur Automation, Leittechniksysteme etc.) und damit einhergehende Schwachstellen und Angriffsvektoren im Zusammenhang mit der Ausnutzung durch einen Bedrohungsakteur betrachtet. Die einzelnen Systeme können dabei Angriffsziele oder auch Angriffswerkzeuge im Rahmen eines Cyberangriffs sein. Bei diesem Ansatz ist der Ausgangspunkt aller Schritte und Betrachtungen die

Gesamtheit aller eingesetzten Systeme, für die jeweils die Risiken abgeleitet werden. Der system-basierte Ansatz setzt somit im Wesentlichen bei Angriffsvektoren im Zusammenhang mit den digitalen Systemen an, die von Angreifern ausgenutzt und zur Herbeiführung von Bedrohungsereignissen eingesetzt werden können. Ebenfalls betrachtet wird die Beeinträchtigung der Systeme durch zufällige Ereignisse. Dabei sind die einzelnen Systeme nicht nur isoliert zu betrachten, sondern auch die Wechselwirkungen und das Gesamtsystem. Als Top-Down-Ansatz werden dabei ausgehend von bestimmten Ursachen mögliche daraus resultierende Konsequenzen betrachtet.

Konsequenz-basierter Ansatz

Ein Konsequenz-basiertes Risk Assessment stellt die Konsequenzen beim Eintritt bestimmter Risiken in den Mittelpunkt des Vorgehens. Konsequenzen umfassen hierbei Auswirkungen oder logische Folgen (Veränderung oder Nicht-Veränderung) eines Ereignisses, eines Vorfalls, einer Handlung oder einer Entscheidung, die in der Regel nicht nur durch das Ereignis, den Vorfall, die Handlung oder die Entscheidung an sich, sondern auch durch die beteiligten Systeme, Menschen und Randbedingungen ermöglicht, erleichtert, verursacht, verhindert, gefördert oder verändert werden kann. Eine Konsequenz kann dabei positiv oder negativ sein.

4.2 Herangehensweise: Qualitativ vs. Quantitativ vs. Semi-quantitativ

Für die Bewertung der Risiken und der zugehörigen relevanten Faktoren wie beispielsweise der Wahrscheinlichkeiten können verschiedene Ansätze gewählt werden. Hierbei wird zwischen qualitativen, quantitativen und semi-quantitativen Bewertungsansätzen unterschieden. Jeder dieser Ansätze besitzt Vor- und Nachteile für die Bewertung eines Risikos, die bei der Entscheidung für einen Bewertungsansatz entsprechend abgewogen werden sollten. /NIS12n01/

Der **qualitative Bewertungsansatz** basiert nicht auf konkreten Berechnungen, sondern schwerpunktmäßig auf definierten Szenarien. Anstatt möglichen Verlusten beim Eintreten der Risiken konkrete Geldwerte oder ein anderes konkretes quantitatives Maß zuzuordnen, werden die Bedrohungen anhand einer Skala eingeordnet, um ihr Risiko, ihre Kosten und ihre Auswirkungen zu bewerten /CIS21b01/. Dabei werden typischerweise eine Reihe von Methoden, Prinzipien oder Regeln angewendet, die auf nicht-nummerischen Kategorien oder Einstufungen (beispielsweise Kategorisierungen wie *sehr niedrig*,

niedrig, *mittel*, *hoch* und *sehr hoch*) basieren /NIS12n01/. Bei der Durchführung der qualitativen Risikoanalyse sind vor allem Urteilsvermögen, Intuition und Erfahrung relevant. Wichtige Techniken für die qualitative Risikoanalyse sind: Brainstorming, Storyboard[2], Fokusgruppen[3], Umfragen, Fragebögen, Checklisten, Einzelgespräche, Interviews, Szenarien und die Delphi-Technik[4]. Welche Techniken angewendet werden, beruht auf der Kultur der Organisation, den Risiken und betroffenen Vermögenswerten (Assets). Üblicherweise werden mehrere unterschiedliche Methoden angewendet und ihre Ergebnisse im abschließenden Risikoanalysebericht verglichen und gegenübergestellt. Die Entwicklung von Szenarien und die Verwendung der Delphi-Technik sind beim qualitativen Bewertungsansatz Standardvorgehensweisen und entsprechend weit verbreitet /CIS21b01/.

Qualitative Ansätze basieren entweder auf deskriptiven (nominalen) oder bewertenden (ordinalen) Skalen[5] der Auswirkungen und der Eintrittswahrscheinlichkeit der Auswirkungen /IEC19n04/. Zur Bewertung der Ausmaße von Auswirkungen und der Eintrittswahrscheinlichkeit der Auswirkungen werden Ordinalskalen mit qualitativen Attributen verwendet, wie beispielsweise *niedrig*, *mittel* und *hoch*. Diese Skalen werden an die gegebenen Umstände angepasst, wobei verschiedene Beschreibungen für unterschiedliche Risiken verwendet werden können /ISO18n03/. Der IT-Grundschutz des BSI nutzt für die Eintrittshäufigkeit beispielsweise die Kategorien *selten*, *mittel*, *häufig* und *sehr häufig* und für die Schadenshöhe *vernachlässigbar*, *begrenzt*, *beträchtlich* und *existenzbedrohend*. Mit den Definitionen der Schadenshöhe und der Eintrittshäufigkeit kann anschließend eine Risikomatrix zur Bewertung der Risiken erstellt werden, die an die eigenen Bedürfnisse angepasst werden kann.

---

[2] zeichnerische Visualisierung eines Vorgangs.

[3] Spezielle moderierte Form der Gruppendiskussion.

[4] Die Delphi Technik ist ein anonymer Feedback- und Antwortprozess, der es einer Gruppe ermöglicht, einen anonymen Konsens zu erreichen. Dabei haben die Experten in mehreren Runden die Möglichkeit ihre ehrliche und unbeeinflusste Antwort zu bestimmten Thesen zu geben.

[5] Bei einer Nominalskala wird ein Merkmal beschrieben und durch Kategorien messbar gemacht, ohne dass dabei eine Reihenfolge festgelegt wird. Bei einer Ordinalskala können die Merkmale bzw. Kategorien auch nach einer Reihenfolge sortiert werden (z.B. sehr hoch, hoch, mittel, niedrig, sehr niedrig).

Mit Hilfe der Risikomatrix können dann qualitative Risikokategorien wie in dem Fall *gering*, *mittel*, *hoch* und *sehr hoch* festgelegt werden /BSI17n02/:

- : Der Angriffspfad kann mit geringem Aufwand erreicht werden.
- **Medium**: Der Angriffspfad kann mit mittlerem Aufwand erreicht werden.
- **Gering**: Der Angriffspfad kann mit hohem Aufwand erreicht werden.
- **Sehr gering**: Der Angriffspfad kann mit sehr hohem Aufwand erreicht werden.

Ein qualitativer Bewertungsansatz kann zunächst verwendet werden, um Risiken zu identifizieren, die eine detaillierte Analyse benötigen. Zudem eignet sich eine qualitative Analyse dann, wenn sie für die Entscheidungen angemessen ist oder wenn die numerischen Daten oder die Mittel für eine quantitative Risikoanalyse unzureichend sind /ISO18n03/. Die Ergebnisse aus dem qualitativen Bewertungsansatz helfen Entscheidungsträgern, die Risiken einzuordnen und zu kommunizieren. Der Wertebereich in den qualitativen Bewertungen ist in den meisten Fällen verhältnismäßig klein und erschwert dadurch die relative Priorisierung oder den Vergleich innerhalb der Menge der identifizierten und bewerteten Risiken. Zusätzlich vertrauen unterschiedliche Experten typischerweise auf ihre individuellen und subjektiven Erfahrungen, sodass dies zu signifikanten Unterschieden in den Ergebnissen der Bewertungen führen kann, vor allem dann, wenn die einzelnen Werte nicht klar definiert oder durch bedeutende Beispiele charakterisiert sind. Die Wiederholbarkeit und Reproduzierbarkeit von qualitativen Bewertungen kann durch die Kommentierung der Werte mit entsprechenden Begründungen für die jeweiligen Einschätzungen und Ergebnisse und durch die definierten Funktionen zur Verbindung der qualitativen Werte erhöht werden. Eine qualitative Risikobetrachtung ist in der Regel praktikabler für die Bewertung der Eintrittshäufigkeit und Schadenshöhe des Risikofalls. Im Allgemeinen werden in der Praxis zunächst qualitative Analysen verwendet, um eine generelle Einschätzung über die Risikohöhe zu erhalten und die Hauptrisiken zu identifizieren. Später kann es notwendig sein, eine spezifischere oder quantitative Analyse des Hauptrisikos durchzuführen, da die Durchführung einer qualitativen Analyse typischerweise weniger komplex und günstiger in der Durchführung als eine quantitative Analyse ist /NIS12n01/.

Durch den Einsatz des **quantitativen Bewertungsansatzes** ergeben sich konkrete Wahrscheinlichkeiten oder anderweitige numerische Angaben des relativen Risikopotenzials, sodass als Endergebnis ein Bericht erstellt werden kann, der Angaben zum Geldwert oder einem anderen quantitativen Maß für die jeweiligen Risiken, den

potenziellen Verlusten, den erforderlichen Gegenmaßnahmen und Sicherheitsvorkehrungen enthält. Ein Vorteil einer quantitativen Analyse ist, dass die entsprechenden Ergebnisse typischerweise anhand von objektiven Kriterien erlangt werden und somit nach objektiven Maßstäben logisch und ohne erweiterte Kenntnisse nachvollziehbar sind. Somit sind die Ergebnisse, beispielsweise in tabellarischer Darstellung, typischerweise für eine breite Personenzahl ersichtlich und verständlich.

Eine rein quantitative Analyse ist jedoch nicht möglich, da einige Elemente und Aspekte der Analyse qualitativ, subjektiv oder anderweitig nach objektiven Maßstäben nicht greifbar sind und somit nicht genau quantifiziert werden können /CIS21b01/. Für den quantitativen Bewertungsansatz gibt es entsprechend eine Reihe von Methoden, Prinzipien und Regeln, die auf numerischen Ansätzen basieren.

Der Prozess der quantitativen Risikobewertung startet mit einer Bewertung der Assets sowie einer Identifikation der korrespondierender Bedrohung. Daraus ergeben sich dann Asset-Bedrohungs-Paare, für die Schätzungen des Schadenspotenzials/Schweregrads und der Häufigkeit/Wahrscheinlichkeit bestimmt werden müssen. Die wesentlichen Schritte der quantitativen Risikoanalyse sind /CIS21b01/:

1. Auflistung der Assets und Zuweisung eines Geldwertes.
2. Herausarbeiten von Bedrohungen für die aufgelisteten Assets, um Asset-Bedrohungs-Paare zu bilden.
3. Berechnung eines Expositionsfaktors (exposure factor, EF) für jedes Paar.
4. Berechnung der Verlusterwartung eines Einzelverlusts (single loss expectancy, SLE) für jedes Paar.
5. Erstellen einer Bedrohungsanalyse für die Wahrscheinlichkeit, dass die Bedrohung innerhalb eines Jahres eintritt (annualized rate of occurence, ARO).
6. Bestimmung des Gesamtschadenspotentials pro Bedrohung durch Berechnung der jährlichen Schadenserwartung (annualized loss expectancy, ALE).
7. Recherchieren und Festlegung von Gegenmaßnahmen für jede Bedrohung und Ermittlung des durch die Gegenmaßnahmen geänderten Expositionsfaktors, der jährlichen Eintrittsrate und der jährlichen Schadenserwartung.
8. Erstellen einer Kosten-Nutzen-Analyse zu jeder Gegenmaßmaßnahme für jede Bedrohung und für jedes Asset. Wahl der geeignetsten Gegenmaßnahme für jede Bedrohung.

Für die Auswirkungen und die Wahrscheinlichkeiten wird eine Skala mit numerischen Werten mit Daten aus einer Vielzahl von Quellen verwendet. Diese Art der Bewertung unterstützt am effektivsten die Kosten-Nutzen-Analysen von alternativen Risikoreaktionen oder Vorgehensweisen /NIS12n01/. Die Qualität dieser Analyse ist abhängig von der Genauigkeit und der Vollständigkeit der numerischen Werte und der Validität der verwendeten Modelle. In den meisten Fällen werden historische Ereignisdaten verwendet, die den Vorteil bieten, dass sie direkt mit den Zielen der Informationssicherheit und den Anliegen einer Organisation in Zusammenhang gebracht werden können /ISO18n03/. Bei der Analyse eines Risikos unter quantitativen Bedingungen sollte sichergestellt werden, dass angemessene Einheiten und Dimensionen genutzt werden.

Das Schadenspotenzial ist unter anderem abhängig von den Annahmen, die über das Vorhandensein und die Effektivität von relevanten Sicherungsmaßnahmen, gemacht werden. Die Bedeutung der quantitativen Resultate ist jedoch nicht immer eindeutig und erfordert gegebenenfalls eine Interpretation und Erklärung, um die Annahmen und Bedingungen zu erläutern, die zu den Ergebnissen geführt haben. Dementsprechend sind für die Auftraggeber bzw. Unternehmen typischerweise Fragen in Bezug auf die Belastbarkeit der Zahlen oder Resultate, die im Bericht des quantitativen Risk Assessment enthalten sind, relevant /IEC19n04/.

Risiken können nicht immer konkret beschrieben werden bzw. ihnen kann nicht immer ein konkreter Wert zugeordnet werden, der die Wahrscheinlichkeit einer bestimmten Auswirkung repräsentiert. Gründe und Beispiele für derartige Situationen, in denen Risiken nicht adäquat angegeben werden können, sind gemäß /IEC19n04/:

- Auswirkungen lassen sich am besten als Wahrscheinlichkeitsverteilung beschreiben.
- Ein Ereignis hat eine Anzahl von verschiedenen Ursachen und führt zu unterschiedlichen Ergebnissen und möglichen Auswirkungen.
- Auswirkungen ergeben sich aus der beständigen Exposition gegenüber einer Risikoquelle.
- Risikoquellen sind identifizierbar, aber die Spezifizierung der genauen Art und die Wahrscheinlichkeit der möglichen Auswirkungen gestaltet sich komplex.

Hinzu kommt, dass typischerweise Informationen verloren gehen, wenn das Ausmaß des Risikos als simples Produkt aus den abgeschätzten Auswirkungen und der Ereigniswahrscheinlichkeit bestimmt wird.

Demnach würde es beispielsweise dadurch keine Unterschiede zwischen Risiken mit hohen Auswirkungen und niedriger Wahrscheinlichkeit und Risiken mit geringen Auswirkungen und hoher Wahrscheinlichkeit geben. Zur Kompensation dessen kann ein Gewichtungsfaktor für die Auswirkungen oder die Wahrscheinlichkeit verwendet werden. Das Zusammenführen von mehreren komplexen Risiken führt zudem zum Informationsverlust über die Komponenten der Risiken. Ein einfaches Aufsummieren von Verteilungsmodellen kann dabei zu falschen Ergebnissen führen, daher sollte die Korrelation zwischen Verteilungsfunktionen beachtet werden /BSI17n02/. In manchen Fällen ist es sinnvoll, Werte von mehreren Risiken zu kombinieren, vorausgesetzt die Risiken sind alle durch eine Auswirkung charakterisiert und in denselben Einheiten gemessen. Eine Kombination ist nur möglich, wenn die Auswirkungen und Eintrittswahrscheinlichkeiten quantitativ bestimmt wurden und die Einheiten einheitlich und korrekt sind /IEC19n04/. Die Art und Weise, in der die Auswirkungen und die Wahrscheinlichkeit ausgedrückt und wie diese kombiniert werden, um eine Risikohöhe zur Verfügung zu stellen, variiert mit der Art des Risikos und dem Ausgang des Ziels des verwendeten Risk Assessments. Die Unsicherheit und die Variation der Auswirkungen und der Wahrscheinlichkeit sollten in der Analyse berücksichtigt und wirksam kommuniziert werden /ISO18n03/.

Eine quantitative Risikobetrachtung ist typischerweise sehr aufwendig und setzt ein umfangreiches statistischen Datenmaterial voraus. Weitere Nachteile, die bei einem quantitativen Ansatz auftreten können, sind die Unverfügbarkeit von überprüfbaren Daten und eine Verringerung der Genauigkeit durch das Einfließen von subjektiven Entscheidungen oder durch eine beträchtliche Unsicherheit bei der Ermittlung der Werte. Die ermittelten Zahlen müssen entsprechend hinterfragt und richtig interpretiert werden, um eine Überschätzung von Ergebnissen wie beispielsweise Genauigkeiten zu vermeiden. Den möglichen Vorteilen einer quantitativen Bewertung in Bezug auf Genauigkeit, Wiederholbarkeit und Reproduzierbarkeit der Bewertungsergebnisse stehen oftmals der Nachteile in Form von hohen Kosten für die Anstellung von Experten, für Arbeitszeit und Arbeitsaufwand sowie die Beschaffung nötiger Werkzeuge gegenüber. Für schwer zu kategorisierende und quantisierende Ereignisse bietet sich eine Kombination aus verschiedenen Verfahren an, um Problemen bei der Analyse von Ereignissen mit schwerwiegenden Auswirkungen in diesem Zusammenhang vorzubeugen /ISO18n04/.

Eine Kombination aus quantitativer und qualitativer Bewertung wird als **semi-quantitativer Bewertungsansatz** bezeichnet. Dieser wendet typischerweise eine Reihe von Methoden, Prinzipien und Regeln an, wie beispielsweise Binning[6], Skalen oder repräsentative Zahlen, deren Werte und Bedeutung nicht in anderen Zusammenhängen enthalten sind. Diese Art der Bewertung kann die Vorteile der quantitativen und qualitativen Bewertung zusammenbringen. Das Binning und die Skalen können leicht in qualitative Bedingungen umgewandelt werden, die eine Kommunikation der Risiken für die Entscheidungsträger unterstützt, während relative Vergleiche zwischen den Werten in verschiedenen oder gleichen Binnings gezogen werden können. Die Rolle einer Expertenbeurteilung bei der Zuweisung der Werte ist ersichtlicher als ein rein quantitativer Ansatz. Wenn die Skalen oder Bins eine ausreichende Granularität bieten, wird die relative Priorisierung unter den Ergebnissen besser unterstützt als bei einem rein qualitativen Ansatz. Jeder Wertebereich muss durch angemessene Beispiele klar definiert und/oder charakterisiert sein. In einigen Situationen ist es sinnvoll, die Risikomaßstäbe als Kombination des Ausmaßes von potenziellen Auswirkungen und der Wahrscheinlichkeit dieser Konsequenzen zur Verfügung zu stellen /NIS12n01/. Dabei schließen semi-quantitative Ansätze ein, dass:

- ein Parameter quantitativ (meistens Wahrscheinlichkeit) ausgedrückt ist und ein anderer Parameter beschrieben oder auf einer Rangskala ausgedrückt ist.
- Skalen in diskrete Bänder unterteilt sind und die Grenzen davon qualitativ ausgedrückt sind. Punkte der Skalen besitzen oft eine logarithmische Beziehung, um an die Daten angepasst werden zu können.
- numerische Beschreibungen zu Skalenpunkten hinzugefügt werden und die Bedeutung dessen qualitativ beschrieben wird.

Die Verwendung von semi-quantitativen Skalen kann zu Missinterpretationen führen, wenn die Basis der Kalkulationen nicht sorgfältig erläutert und beschrieben wurde. Deshalb sollte ein semi-quantitativer Ansatz stets validiert und ausschließlich nach entsprechend sorgfältiger Überprüfung verwendet werden /IEC19n04/.

[6] Häufigkeitsverteilung einer Stichprobe mittels eines Histogramms/Balkendiagramms.

Es gibt zahlreiche Einflussfaktoren eines Risk Assessments, die berücksichtigt, dokumentiert und kommuniziert werden müssen. Darunter fallen unterschiedliche Meinungen, Voreingenommenheit, Risikowahrnehmungen, Beurteilungen, die Qualität der verwendeten Informationen, getroffene Annahmen und Ausschlüsse, sowie Beschränkungen und Art der Ausführungen dieser Verfahren. Die Abschätzung der Wahrscheinlichkeiten kann abhängig vom Kontext variieren /ISO18n04/.

Qualitative und semi-quantitative Techniken dürfen lediglich für den Vergleich von Risiken mit anderen Risken, die auf die gleiche Art und Weise bemessen oder mit den gleichen Kriterien ausgedrückt wurden, verwendet werden. Die oben genannten Techniken können nicht direkt verwendet werden, um Risiken miteinander in Verbindung zu setzen oder zusammenzufassen. Zudem ergeben sich möglicherweise Probleme in Bezug auf die Anwendbarkeit bei der Anwendung in Situationen, in denen es positive und negative Auswirkungen gibt oder Abwägungen/Kompromisse zwischen Risiken gemacht werden. Eine Gruppe von qualitativ oder semi-quantitativ bestimmten Risiken kann nicht direkt zusammengefügt werden.

4.3 Blickrichtung: Top-down vs. Bottom-up

Bei einem **top-down Ansatz** werden grundsätzlich Ursachen wie Bedrohungsereignisse, Bedrohungsquellen oder Schwachstellen betrachtet, die zu bestimmten Auswirkungen führen können. Beispiele für top-down Ansätze im Rahmen eines Risk Assessments sind der Bedrohungs-basierte, der System-basierte und der Schwachstellen-basierte Ansatz (siehe Abschnitt 4.1). So werden zu Beginn Bedrohungsquellen und Bedrohungsereignisse identifiziert oder es wird mit einer Reihe von prädisponierten Bedingungen, Schwachstellen oder Anfälligkeiten des organisatorischen Umfelds oder der eingesetzten Systeme gestartet. Darauf aufbauend werden Bedrohungsszenarien entwickelt. Bei diesem Ansatz werden also ausgehend von Bedrohungen oder Schwachstellen die resultierenden Auswirkungen bestimmt. Beispielsweise wird eine bestimmte Bedrohung/Schwachstelle betrachtetet bzw. identifiziert und daraus abgeleitet, welche Konsequenzen aus dieser Bedrohung oder der Ausnutzung dieser Schwachstelle hervorgehen könnten.

Im Gegensatz zu dem top-down Ansatz steht der **bottom-up Ansatz**, bei dem ausgehend von den potenziellen Auswirkungen die entsprechenden Ursachen identifiziert werden.

Ein Beispiel für den bottom-up Ansatz stellt der konsequenz-basierte Ansatz dar (siehe Abschnitt 4.1). Demnach wird mit der Identifizierung von potenziellen, meist unerwünschten Auswirkungen begonnen und ausgehend von den bestimmten Auswirkungen evaluiert, welche Bedrohungen, Schwachstellen oder Angriffsvektoren für eine bestimmte Auswirkung ursächlich sein können.

Bei einem top-down Ansatz ist das Ziel somit, die potenziellen Auswirkungen ausgehend von den zuvor bestimmten Ursachen zu ermitteln. Bei einem bottom-up Ansatz wird ausgehend von den potenziellen Auswirkungen auf die entsprechenden Ursachen geschlossen.

5 Entwicklung einer generischen Vorgehensweise

Das Risk Assessment insgesamt stellt nach der Kontextualisierung von Risiken einen Schritt im Risk Management Prozess dar, an den sich dann der Schritt der Risiko-Behandlung anschließt, in dem der weitere Umgang mit den Risiken geplant wird. Zur Entwicklung einer generischen Vorgehensweise ist daher die Betrachtung des gesamten Risk Management Prozesses wesentlich.

Die Entwicklung einer generischen Vorgehensweise für die Durchführung eines Risk Managements für schutzbedürftige IT-Systeme in kerntechnischen Anlagen und Einrichtungen stützt sich zunächst auf die Betrachtung der vier unterschiedlichen Ansätze für das Risk Management. Aufbauend auf die spezifische Beschreibung der einzelnen Schritte im Rahmen des Risk Managements und die Diskussion der Unterschiede in der Herangehensweise sowie der Vor- und Nachteile der einzelnen Ansätze (siehe Abschnitt 5.1) werden die relevanten Aspekte im Hinblick auf kerntechnische Anlagen und Einrichtungen herausgearbeitet (siehe Abschnitt 5.2). Weiterhin werden spezielle Aspekte in Bezug auf Wiederholung und Überprüfung eines Risk Assessments diskutiert. Darauf aufbauend wird eine generische Vorgehensweise für deutsche kerntechnische Anlagen und Einrichtungen entwickelt (siehe Abschnitt 5.3), wobei zunächst Kernkraftwerke betrachtet und anschließend die Übertragung der Prozessschritte auf Zwischenlager und Anlagen der SK III diskutiert werden.

5.1 Beschreibung ausgewählter Vorgehensweisen

Die wichtigsten Aspekte des Risk Assessment umfassen die Identifikation und Einschätzung von Risiken. Wie in Kapitel 3 dargestellt, gibt es in den verschiedenen nationalen und internationalen Standards eine ganze Reihe von Unterschieden bei den einem Risk Assessment zugrunde liegenden Prozessen, ebenso im Rahmen des Risk Management, welches das Risk Assessment umfasst. Als Grundlage für die Entwicklung einer generischen Vorgehensweise werden zunächst, in Übereinstimmung mit der Mehrzahl der oben beschriebenen Standards, die wesentlichen Prozessschritte beim Risk Assessment und Risk Management definiert. Anschließend werden die vier in Kapitel 4 beschriebenen Ansätze (Schwachstellen-basiert, Bedrohungs-basiert, Konsequenz-basiert, System-basiert) anhand dieser Prozessschritte beschrieben.

5.1.1 Prozessschritte bei Risk Assessment und Risk Management

Bei allen Vorgehensweisen beim Risk Assessment werden hierzu im Wesentlichen immer drei Schritte durchgeführt:

- Risiko-Identifizierung
- Risiko-Analyse
- Risiko-Evaluation

Im Rahmen des Risk Managements wird das Risk Assessment in weitere Prozessschritte eingebettet:

- Risiko-Kontextualisierung
- Risk Assessment mit den oben genannten Prozessschritten
- Risiko-Behandlung einschließlich Definition bzw. Anpassung von (zusätzlichen) Sicherungsmaßnahmen

Der Prozess des Risk-Assessments erfordert eine regelmäßige Wiederholung, um sich ändernde Risiken zu erfassen und entsprechende Vorgehensweisen und Maßnahmen anzupassen.

Die Kontextualisierung der Risiken erfolgt unabhängig vom gewählten Ansatz und wird in Abschnitt 4.2 mitbetrachtet.

5.1.2 Schwachstellen-basierter Ansatz

Im Folgenden werden die oben genannten einzelnen Schritte des schwachstellen-basierten Risk-Assessments näher erläutert. Als Top-Down-Ansatz werden dabei ausgehend von bestimmten Ursachen mögliche daraus resultierende Auswirkungen betrachtet.

Risiko-Identifizierung

Das Ziel der Risiko-Identifizierung ist generell die Identifizierung relevanter Risiken in Bezug auf Sicherheits- und Sicherungsaspekte der eingesetzten IT-Systeme und Komponenten. Beim schwachstellen-basierten Ansatz geht es dabei zunächst um die Identifizierung von Schwachstellen beispielsweise in IT-Systemen, Prozessen oder Sicherungsmaßnahmen sowie Angriffsvektoren zur Ausnutzung dieser Schwachstellen. Davon ausgehend geht es um die Identifizierung von Bedrohungen, die diese identifizierten Schwachstellen mittels der identifizierten Angriffsvektoren ausnutzen könnten, wobei ebenfalls sowohl neue als auch Änderungen bereits bekannter Bedrohungen betrachtet werden sollen. Die Risiken ergeben sich aus einer möglichen Ausnutzung der Schwachstellen durch die Bedrohungen, wobei es sich entweder um absichtliche Angreiferhandlungen als auch um eine Ausnutzung durch zufällige Ereignisse handeln kann. Bei diesem Schritt sollen nicht nur neue bzw. zusätzliche, sondern auch Änderungen bereits erkannter Risiken erfasst werden wie beispielsweise weitere Möglichkeiten zur Ausnutzung bekannter Schwachstellen. Die Risiko-Identifizierung umfasst die Durchführung dieses Vorgehens für alle sicherheits- oder sicherungsrelevanten Komponenten und IT-Systeme. Alle Betrachtungen sollten insbesondere hinsichtlich der Relevanz und Wichtigkeit des einzelnen IT-Systems für die Sicherheit und Sicherung durchgeführt werden.

Risiko-Analyse

Die Risiko-Analyse greift die im vorigen Schritt identifizierten Risiken auf, wobei diese analysiert und hinsichtlich der Einschätzung des Risikos betrachtet werden. Zentral ist dabei die Analyse aller identifizierten Schwachstellen, Angriffsvektoren und der zugehörigen Bedrohungen hinsichtlich potenzieller Folgen der jeweiligen Ausnutzung. Dies umfasst zunächst die Betrachtung möglicher Auswirkungen ausgehend von den jeweiligen Angriffsvektoren unter Berücksichtigung entsprechender Bedrohungsszenarien und Ausnutzung von Schwachstellen. Darauf aufbauend ist für alle Risiken und die korrespondierenden potenziellen Auswirkungen zu bestimmen, mit welcher Wahrscheinlichkeit der Risikofall eintritt. Dies kann quantitativ, qualitativ beispielsweise in abgestufter Form von „sehr gering“ bis „sehr hoch“, sowie semi-qualitativ/quantitativ erfolgen. Daraus ergeben sich entsprechende Entscheidungen, welche der potenziellen Auswirkungen relevant sind und im Rahmen des Risiko-Managements weiter berücksichtigt werden müssen und welche möglichen Auswirkungen vermieden oder falls dies nicht möglich ist, mitigiert werden müssen.

Bei der Einschätzung der identifizierten Risiken müssen zunächst die Wahrscheinlichkeit des Eintritts des Risikofalls und die Schwere der potenziellen Auswirkungen bei Eintreten des Risikofalls bestimmt werden. Die entsprechende Risikostufe ergibt sich aus der Eintrittswahrscheinlichkeit und der zugehörigen Auswirkungen des jeweiligen Risikos. Dieser Prozess kann je nach genauen Umständen mit erheblichen Unsicherheiten belastet sein, insbesondere da eine Quantifizierung der für die Risiken relevanten Parameter typischerweise nicht oder nur eingeschränkt möglich ist.

Risiko-Evaluierung

Bei der Risiko-Evaluierung wird sorgfältig geprüft, wie gut eine Anlage gegen die aus den jeweiligen Schwachstellen hervorgehenden, identifizierten Risiken geschützt ist. Für jedes identifizierte Risiko ist dabei zu bewerten, ob ein angemessener Schutz vorhanden ist, beispielsweise durch die definierten Sicherungsmaßnahmen. Dabei können bereits etablierte oder geplante technische, administrative oder personelle Sicherungsmaßnahmen kreditiert werden, wobei der Schwerpunkt des Blickwinkels in Anbetracht des Schwachstellen-basierten Ansatzes bei der Informationssicherheit liegen sollte. Die etablierten und geplanten Sicherungsmaßnahmen sollten das entsprechende Risiko widerspiegeln und alle Defizite hinsichtlich des Schutzes einzelner IT-Systeme gegen ein bestimmtes Risiko sind dabei zu identifizieren, sodass alle damit in Zusammenhang stehenden IT-Systeme mit Schwachstellen in der Informationssicherheit identifiziert werden.

Risiko-Behandlung

Nach der Identifizierung von Defiziten bezüglich bestimmter identifizierter Risiken werden im letzten Schritt für alle betroffenen Risiken und Systeme Maßnahmen zur Risiko-Behandlung erwogen. Hierzu zählt insbesondere die Definition zusätzlicher bzw. Anpassung bereits etablierter Sicherungsmaßnahmen. Dabei sind diese Sicherungsmaßnahmen so auszuwählen, dass dadurch die Informationssicherheit für das jeweilige identifizierte Risiko erhöht wird. Dies kann sowohl einzelne Maßnahmen wie auch ganze Prozesse (beispielsweise im Rahmen des Patch- und Updatemanagements) umfassen. Generell müssen die zusätzlich definierten Sicherungsmaßnahmen hinsichtlich der Aspekte Sicherheit, Sicherung und Betrieb ausgewählt werden und dürfen nicht mit den bereits im früheren Prozess des Risk-Assessments betrachteten Maßnahmen kollidieren. Eventuelle Konflikte und Rückwirkungen müssen entsprechend geprüft und gegebenenfalls beseitigt werden.

Über die Definition von Sicherungsmaßnahmen hinaus gibt es noch weitere Handlungsmöglichkeiten im Rahmen der Risiko-Behandlung. Gerade beim schwachstellen-basierten Ansatz stellt sich hierbei vor allem die Frage nach einer möglichen Risiko-Vermeidung, also einer Behebung der identifizierten Schwachstellen.

5.1.3 Bedrohungs-basierter Ansatz

Risiko-Identifizierung

Bei der Verwendung eines bedrohungs-basierten Ansatzes für das Risk Assessment wird das Risiko auf Grundlage der entwickelten Bedrohungsszenarien ermittelt. Daher müssen in einem ersten Schritt die Bedrohungen (Bedrohungsquellen und Bedrohungsereignisse) für alle IT-Systeme und ihre Komponenten identifiziert werden. Bei diesem Vorgehen sollten alle sicherheits- und sicherungsrelevanten Komponenten und IT-Systeme berücksichtigt werden. Anschließend werden auch Schwachstellen und Angriffsvektoren und dadurch konkrete Angriffsszenarien bzw. Szenarien in Zusammenhang mit zufälligen Ereignissen identifiziert, die möglicherweise von einer Bedrohung genutzt werden können. Die Risiken ergeben sich aus einer möglichen Ausnutzung der Schwachstellen durch die Bedrohungen, wobei es sich entweder um absichtliche Angreiferhandlungen als auch um eine Ausnutzung durch zufällige Ereignisse handeln kann.

Risiko-Analyse

Bei der Analyse der zuvor identifizierten Bedrohungen und entwickelten Bedrohungs- und Angriffsszenarien werden diese auf ihre potenziellen Auswirkungen hin überprüft. Dabei wird angenommen, dass bestehende, neue oder veränderte Schwachstellen und Angriffsvektoren von der Bedrohung genutzt werden. Bei der Auswirkungsanalyse dienen die Bedrohungsquelle, das Bedrohungsereignis und die Szenarien als Grundlage. Daher stehen bei einem Bedrohungs-basierten Ansatz die Absichten des Angreifers und seine maliziösen Handlungen im Vordergrund und bestimmen die Auswirkungen der Bedrohungen (z. B. durch seine Fähigkeiten, sein Vorgehen, seine Kapazitäten etc.). Für alle Bedrohungen ist dann das Ausmaß des zu erwartenden Schadens zu bestimmten. Dabei kann ein qualitativer, quantitativer oder semi-qualitativer/quantitativer Ansatz gewählt werden, um das Ausmaß zu bewerten.

Nach der Bewertung der Auswirkungen der Szenarien sollte auch die Eintrittswahrscheinlichkeit für das Szenario abgeschätzt werden.

Mit der Bestimmung der Eintrittswahrscheinlichkeit in Kombination mit den Auswirkungen der Szenarien, kann das Risiko abgeschätzt werden. Da eine Quantifizierung der für die Risiken relevanten Parameter wie beispielsweiser der zukünftigen Angreifermotivation zumeist nur sehr eingeschränkt möglich ist, kann die Ermittlung eines Risikos häufig nur mit großen Unsicherheiten erfolgen.

Risiko-Evaluierung

Bei der Risiko-Evaluierung wird ähnlich wie beim Schwachstellen-basierten Ansatz vorgegangen. Dabei wird sorgfältig geprüft, wie gut eine Anlage gegen die aus den Bedrohungen hervorgehenden und identifizierten Risiken geschützt ist. Alle etablierten oder geplanten technischen, administrativen oder personellen Sicherungsmaßnahmen werden dabei kreditiert. Unter Berücksichtigung aller Maßnahmen sind mögliche Defizite beim Schutz der IT-Systeme zu identifizieren.

Risiko-Behandlung

Nach dem Schritt der Risiko-Evaluierung ergeben sich entsprechende Entscheidungen, welche Bedrohungen als relevant eingeschätzt und im Rahmen der Risiko-Behandlung weiter berücksichtigt werden müssen. Schwerwiegende Auswirkungen müssen vermieden oder mitigiert werden, beispielsweise durch die Definition zusätzlicher Sicherungsmaßnahmen. Die Definition zusätzlicher Sicherungsmaßnahmen erfolgt bei allen Ansätzen gleich. In diesem Schritt werden zuerst Defizite in Bezug auf die identifizierten Risiken ermittelt. Danach werden für alle betroffenen Risiken und Systeme zusätzliche Sicherheitsmaßnahmen definiert. Im Unterschied zum Schwachstellen-basierten Ansatz, der unter Umständen erlaubt, Schwachstellen im Rahmen der Risiko-Behandlung direkt zu beheben, besteht diese Option bei Bedrohungen nicht. Diese lassen sich grundsätzlich durch das Ergreifen von Sicherungsmaßnahmen nicht beeinflussen.

5.1.4 Konsequenz-basierter Ansatz

Risiko-Identifikation

Die Risiko-Identifikation besteht aus mehreren Teilschritten. Zunächst müssen die relevanten Konsequenzen identifiziert werden. Im Kontext des Risk Assessments sind dies vornehmlich unerwünschte Konsequenzen, die es zu vermeiden oder mitigieren gilt. Davon ausgehend werden Angriffsvektoren und Schwachstellen identifiziert, deren

Ausnutzung zu den unerwünschten Konsequenzen führen könnten. Abschließend werden Bedrohungen identifiziert, die potenziell diese Angriffsvektoren umsetzen und die Schwachstellen ausnutzen könnten. Die Risiken ergeben sich wie bei den anderen Ansätzen aus einer möglichen Ausnutzung der Schwachstellen durch die Bedrohungen, wobei es sich entweder um absichtliche Angreiferhandlungen als auch um eine Ausnutzung durch zufällige Ereignisse handeln kann. Da der konsequenz-basierte Ansatz von den möglichen Konsequenzen ausgehend ihre möglichen Ursachen betrachtet, ist er im Unterschied zu den anderen drei betrachteten Ansätzen ein bottom-up Ansatz.

Risiko-Analyse

Jede der identifizierten relevanten Konsequenzen muss analysiert werden, um alle Schwachstellen und Angriffsvektoren zu ermitteln, deren Nutzung zu der entsprechenden Konsequenz führen können. Im darauffolgenden Schritt werden Bedrohungen, die möglicherweise die identifizierten Angriffsvektoren nutzen oder die ermittelten Schwachstellen ausnutzen können, bestimmt. Jedes der identifizierten Risiken wird quantitativ oder qualitativ eingeordnet, wobei der Schweregrad der potenziellen Konsequenzen und deren Eintrittswahrscheinlichkeit berücksichtigt werden.

Risiko-Evaluierung

Bei der Risiko-Evaluierung wird analog zu den anderen Ansätzen überprüft, wie gut die Anlage gegen die aus den Konsequenzen ermittelten Schwachstellen und Angriffsvektoren geschützt ist. Für jedes identifizierte Risiko ist dabei zu bewerten, ob die betroffenen IT-Systeme durch definierte Sicherungsmaßnahmen etc. ausreichend geschützt sind.

Risiko-Behandlung

Die Risiko-Behandlung erfolgt analog zu den anderen Ansätzen. Es werden unter anderem Defizite in Bezug auf die identifizierten Risiken ermittelt, für die dann zusätzliche Sicherheitsmaßnahmen definiert oder bestehende Sicherungsmaßnahmen angepasst werden.

Durch Sicherungsmaßnahmen lassen sich unerwünschte Konsequenzen nicht vollständig eliminieren, allerdings lassen sich in vielen Fällen die Eintrittswahrscheinlichkeiten für die Konsequenzen herabsetzen oder auch das mit den Konsequenzen verbundene Schadensausmaß verringern.

5.1.5 System-basierter Ansatz

Risiko-Identifizierung

Die Risiko-Identifizierung dient zur Identifizierung relevanter Risiken in Bezug auf Sicherheits- und Sicherungsaspekte der eingesetzten Systeme und Komponenten. Das Ziel ist dabei die Identifizierung von Bedrohungen auf der Basis der einzelnen Systeme und Komponenten sowie des Gesamtsystems. Die Risiko-Identifizierung umfasst die Durchführung dieses Vorgehens für alle sicherheits- oder sicherungsrelevanten Komponenten und Systeme. Alle Betrachtungen sollten insbesondere hinsichtlich der Relevanz und Wichtigkeit des einzelnen Systems und des Gesamtsystems für die Sicherheit und Sicherung durchgeführt werden.

Risiko-Analyse

Die Risiko-Analyse umfasst zunächst die Betrachtung möglicher Auswirkungen ausgehend von den jeweiligen Angriffsvektoren. Dabei werden entsprechende Bedrohungsszenarien berücksichtigt, die von einzelnen Systemen bzw. mehreren Systemen ausgehen. Zur Durchführung dieser Schritte für jede Schwachstelle und jeden Angriffsvektor, die für sicherheits- und sicherungsrelevante Systeme identifiziert wurden, müssen alle relevanten Aspekte im Zusammenhang mit den jeweiligen Systemen berücksichtigt werden. Dabei ist insbesondere zu betrachten, inwieweit andere, für die Sicherheit oder Sicherung relevante Systeme durch mögliche manipulierte, fehlerhafte oder ausbleibende Daten des betreffenden Systems beeinträchtigt werden. Entsprechende Sicherheitsanalysen und andere Dokumente, die Informationen über zu vermeidende oder nicht akzeptable Auswirkungen in Bezug auf die vom System ausgeführten Funktionen oder Dienste geben, sind dabei einzubeziehen.

Die Bestimmung des Schweregrads der Auswirkungen der Kompromittierung bestimmter Systeme kann dazu führen, dass der Schutzbedarf der Systeme hinsichtlich der Informationssicherheit entsprechend angepasst werden muss.

Bei der Zuordnung von Risikostufen über eine quantitative oder qualitative Einordnung aller identifizierten Risiken müssen zunächst die Wahrscheinlichkeiten des Eintritts des Risikos und der Schweregrad der Auswirkungen nach Eintreten des Risikos bestimmt werden. Daraus muss eine Gesamtwahrscheinlichkeit für das Eintreten des Risikos und daraufhin des darauffolgenden Schadensfalls bestimmt werden. Die entsprechende Risikostufe ergibt sich aus der Eintrittswahrscheinlichkeit und der zugehörigen Auswirkungen des jeweiligen Risikos. Bereits etablierte oder geplante Sicherungsmaßnahmen sind bei der Ermittlung der Risikostufe nicht zu berücksichtigen.

Risiko-Evaluation

Bei der Risiko-Evaluation wird evaluiert, wie gut eine Organisation gegen die im Zusammenhang mit den betrachteten Systemen identifizierten Risiken geschützt ist. Für jedes identifizierte Risiko ist dabei zu bewerten, ob die betroffenen Systeme angemessen gegen die jeweiligen Risiken geschützt sind, beispielsweise durch die definierten Sicherungsmaßnahmen. Dabei können bereits etablierte oder geplante technische, administrative oder personelle Sicherungsmaßnahmen kreditiert werden.

Risiko-Behandlung

Nach der Identifikation von Defiziten bezüglich bestimmter identifizierter Risiken werden im letzten Schritt für alle betroffenen Risiken und Systeme zusätzliche Sicherungsmaßnahmen definiert. Dabei sind diese Sicherungsmaßnahmen so auszuwählen, dass dadurch die Informationssicherheit für das jeweilige identifizierte Risiko erhöht wird. Dies kann sowohl einzelne Maßnahmen wie auch ganze Prozesse umfassen. Generell müssen die zusätzlich definierten Sicherungsmaßnahmen hinsichtlich der Aspekte Sicherheit, Sicherung und Betrieb ausgewählt werden und dürfen nicht mit den bereits im früheren Prozess des Risk-Assessments betrachteten Maßnahmen kollidieren. Eventuelle Konflikte und Rückwirkungen müssen entsprechend geprüft und gegebenenfalls beseitigt werden. Da es im Entscheidungsbereich einer Organisation liegt, welche IT-Systeme konkret eingesetzt werden und wie mit Schwachstellen dieser Systeme umgegangen wird, bestehen hier weitere direkte Einflussmöglichkeiten im Rahmen der Risiko-Behandlung.

5.1.6 Diskussion

Die oben genannten ausgewählten Vorgehensweisen in Bezug auf die Durchführung eines Risk-Assessments weisen jeweils unterschiedliche Vor- und Nachteile auf und sind je nach den genauen Umständen geeignet, weniger geeignet oder ungeeignet für die Erfassung und den späteren Umgang mit Risiken. Im Folgenden werden die vorgestellten Herangehensweisen in Bezug auf die jeweiligen Stärken und Schwächen sowie anhand unterschiedlicher relevanter Kriterien wie beispielsweise dem Fokus und der Anwendbarkeit verglichen und insbesondere hinsichtlich der Eignung im Rahmen des Vorhabens diskutiert.

Hinsichtlich der grundlegenden Perspektive der verschiedenen Ansätze gibt es zunächst jeweils grundlegende Unterschiede. Der System- und der Schwachstellen-basierte Ansatz gehen von den vorhandenen und eingesetzten Systemen aus und konzentrieren sich dabei beispielweise auf die konkret eingesetzten Systeme, die etablierten Prozesse und die realisierten Sicherungsmaßnahmen sowie auf bekannte technische Schwachstellen in Systemen, Software und Konfigurationen. Dabei wird das sicherheitsrelevante Systemverhalten bzw. das Verhalten einzelner Komponenten betrachtet, um das einzelne System bzw. das Gesamtsystem gegen ausnutzbare Sicherheitslücken, Schwachstellen und anderweitige Defizite abzusichern und zu schützen. Die Betrachtung liegt also im Wesentlichen zunächst bei den eigenen Systemen und den sich in diesem Zusammenhang ergebenden Risiken (top-down Betrachtung). Der konsequenz-basierte Ansatz legt dagegen den Blick im Rahmen einer bottom-up Betrachtung auf Risiken auf Basis potenzieller unerwünschter Auswirkungen eines erfolgreichen Angriffs auf Prozesse und Systeme. Auch in diesem Fall liegen die eigenen Systeme grundsätzlich im Fokus des Ansatzes, jedoch aus Sicht der potenziellen Konsequenzen und ihrer Rolle in den hierfür relevanten Angriffsvektoren. Der bedrohungs-basierte Ansatz setzt dagegen zunächst bei potenziellen externen Bedrohungsakteuren und Bedrohungen an, und analysiert dabei entsprechende Fähigkeiten, Absichten, Methoden und Motive, um realistische Angriffsszenarien und daraus resultierende Risiken zu bewerten. Der Fokus liegt somit zunächst auf externen Gegebenheiten.

Als Ausgangspunkt für den Schwachstellen- und den System-basierten Ansatz dienen dabei beispielsweise Informationen über die eigenen IT-Systeme, insbesondere hinsichtlich des Aufbaus, der Strukturierung und der Vernetzung, sowie in Bezug auf Konfigurations- und Patch-Zustände der Systeme.

Gegebenenfalls können diesbezüglich relevante Informationen mit Hilfe von Softwareanwendungen (wie beispielsweise Schwachstellen-Scannern) erhoben werden. Für den Konsequenz-basierten Ansatz sind insbesondere gesetzliche Vorgaben, Erkenntnisse aus Business-Impact-Analysen und anderweitigen Betrachtungen in Bezug auf potenzielle Konsequenzen entsprechender Risiken als Ausganspunkt relevant. Der Bedrohungs-basierte Ansatz baut im Wesentlichen zunächst auf Informationen zu Bedrohungslage und relevanten Bedrohungsakteuren auf, wobei die jeweiligen Angreifermotivationen, Methoden und auch historische Angriffsdaten betrachtet werden.

In Hinsicht auf die Bewertung potenzieller Risiken gibt es wesentliche Unterschiede zwischen den einzelnen Ansätzen, sowohl in Bezug auf qualitative als auch quantitative Aspekte. Beim Schwachstellen-basierten Ansatz erfolgt die Bewertung typischerweise über standardisierte und somit vergleichbare quantitative Größen, die sich beispielsweise aus den Eigenschaften der Schwachstellen ergeben. Hierzu zählen unter anderem der Schweregrad und die Ausnutzbarkeit bzw. Verfügbarkeit entsprechender Exploits. Im Rahmen des system-basierten Ansatzes liegen bezüglich der Bewertung potenzieller Risiken oftmals Modellierungen oder modellbasierte Methoden zugrunde, um beispielsweise Systemreaktionen und Auswirkungen bei Angriffen und Fehlern zu betrachten. Der konsequenz-basierte Ansatz ist typischerweise durch eine qualitative oder semi-qualitative Herangehensweise bei der Bewertung der Risiken gekennzeichnet, wobei wesentliche Faktoren die Schadenshöhe bei Eintritt und die Eintrittswahrscheinlichkeit des Risikos sind. Der Bewertung bei dem bedrohungs-basierten Ansatz liegen im Wesentlichen mit der Bedrohung zusammenhängende externe Faktoren zugrunde, unter anderem Annahmen in Bezug auf Wahrscheinlichkeiten für einen Angriff, Fähigkeiten der entsprechenden Akteure und der potenziellen Auswirkungen.

Neben den oben genannten Unterschieden in Bezug auf die unterschiedlichen Perspektiven, Ausgangspunkte und Bewertungen sind die verschiedenen Ansätze jeweils von unterschiedlichen Stärken und Schwächen gekennzeichnet:

- Der **Schwachstellen-basierte Ansatz** bietet beispielsweise oftmals eine schnelle und konkrete Grundlage für die Einschätzung technischer Schwachstellen und mögliche Absicherungen und Prioritäten bei dem Umgang mit diesen, wobei jedoch typischerweise die realen Angriffswahrscheinlichkeiten oder die Bedeutung der einzelnen Systeme nicht vollumfänglich betrachtet werden bzw. im Vordergrund stehen. Dadurch, dass der schwachstellen-basierte Ansatz vollständig von der Kenntnis der Schwachstellen und Anfälligkeiten abhängt und somit noch nicht bekannt

gewordene Schwachstellen nicht berücksichtigen kann, liefert ein Risk Assessment, welches sich allein auf einen schwachstellen-basierten Ansatz stützt, zwangsläufig ein unvollständiges Bild der tatsächlichen Risiken.

- Der **System-basierte Ansatz** ist typischerweise durch eine ganzheitliche und strukturierte Vorgehensweise in Bezug auf alle vorhandenen Systeme gekennzeichnet, wobei entsprechend alle damit einhergehenden Risiken berücksichtigt werden. Der Modellierungsaufwand ist dementsprechend hoch und die Durchführung ggf. komplex, wobei auch ein tiefgehendes Systemverständnis erforderlich ist. Der system-basierte Ansatz ist in der Lage, ein deutlich umfassenderes Bild der tatsächlichen Risiken zu zeichnen, als es ein schwachstellen-basierter Ansatz kann. Allerdings muss auch beim system-basierten Ansatz davon ausgegangen werden, dass nicht alle Risiken vollständig erfasst werden. Dies liegt im Wesentlichen an der auf Einzelsysteme fokussierten Betrachtung und der dadurch häufig nicht vollständigen Berücksichtigung aller Zusammenhänge und Wechselwirkungen der einzelnen Systeme. Ein weiterer Einflussfaktor ist die ggf. nicht vollständige Erfassung aller relevanten Systeme.
- Der **Konsequenz-basierte Ansatz** erlaubt durch die Auswahl von und Fokussierung auf einzelne, unerwünschte Konsequenzen eine gezielte Identifikation und Analyse der mit diesen Konsequenzen verbundenen Risiken, Angriffsvektoren und Systeme. Dadurch zeichnet der Konsequenz-basierte Ansatz für die betrachteten Konsequenzen ein im Vergleich zu den anderen drei Ansätzen vollständigeres Bild der tatsächlichen Risiken, wobei der Aufwand in Bezug auf diese Konsequenzen geringer ausfällt als beim system-basierten Ansatz. Allerdings kann der konsequenz-basierte Ansatz keine Aussagen zu den nicht betrachteten Konsequenzen machen. Eine systematische Betrachtung aller unerwünschter Konsequenzen führt beim Konsequenz-basierten Ansatz zu einem ähnlich hohen Modellierungsaufwand und einer ggf. komplexen Durchführung wie die Betrachtung aller Systeme beim System-basierten Ansatz. Beim Konsequenz-basierten Ansatz ergibt sich einhergehend mit der Durchführung zusätzlich eine gewisse Priorisierung der Risiken, die im weiteren Verlauf des Risikomanagements berücksichtigt werden kann. Dabei liegt der Fokus typischerweise im Bereich geschäftsrelevanter Faktoren wie beispielsweise Business Continuity, wobei technische Einzelheiten ggf. vernachlässigt werden.

- Der **Bedrohungs-basierte Ansatz** liefert im Wesentlichen eine von der aktuellen IT-Bedrohungslage geprägte Einschätzungen durch die Blickweise aus der Angreiferperspektive, sodass relevante Angriffsszenarien analysiert werden können. Hierbei ergibt sich typischerweise ein hoher Aufwand zur Erfassung und Analyse der relevanten Bedrohungen, wobei die Qualität und Aktualität der Bedrohungsdaten ein kritischer Faktor für den Erfolg des Ansatzes ist. Dabei wird ggf. neben objektiven Fakten auch auf subjektive Einschätzungen zurückgegriffen. Durch die dynamische Entwicklung der IT-Bedrohungslage ergibt sich bei einem Bedrohungs-basierten Risk Assessment häufig die Notwendigkeit einer Überprüfung oder Wiederholung einzelner Risk Assessment Schritte. Dadurch, dass zwangsläufig nicht alle Bedrohungen in allen relevanten Einzelheiten bekannt sind, kann bei alleiniger Anwendung eines Bedrohungs-basierten Risk Assessments kein vollständiges Bild der tatsächlichen Risiken erfasst werden.

Insgesamt ergeben sich somit unterschiedliche Vor- und Nachteile in Bezug auf die unterschiedlichen Ansätze. Für ein möglichst vollständiges Bild und zur Vermeidung von nicht abgedeckten Bereichen beim Risk Assessment ist es daher sinnvoll, mehrere Herangehensweisen zu berücksichtigen. Dabei sollten möglichst bei der Bewertung von Risiken qualitative und quantitative Aspekte berücksichtigt werden. Zudem sollten beide oben diskutierte Blickrichtungen (top-down und bottom-up) bei der Durchführung eingesetzt werden.

Um die mit dem eigenen System einhergehenden Risiken zu betrachten sind zunächst der Schwachstellen- und der System-basierte Ansatz am geeignetsten, da diese von den eingesetzten Systemen und ggf. vorhanden Schwachstellen ausgehen. Da die Schwachstellen eines Systems auch in die Analysen des system-basierten Ansatzes einfließen und dieser typischerweise einen breiteren Betrachtungswinkel als der Schwachstellen-basierte Ansatz aufweist, ist es bei der Entwicklung einer generischen Vorgehensweise zunächst hinreichend, bezüglich des Ausgangspunktes der eigenen Systeme den System-basierten Ansatz heranzuziehen und dabei das Vorliegen von relevanten Schwachstellen zu unterstellen. Um neben der Blickrichtung ausgehend von den eigenen Systemen (top-down) auch die komplementäre Sichtweise abzudecken und in Bezug auf ausgewählte, unerwünschte Konsequenzen ein möglichst vollständiges Bild der tatsächlichen Risiken zu erhalten, eignet sich der Konsequenz-basierte Ansatz (bottom-up). Daher wird dieser bei der Entwicklung einer generischen Vorgehensweise als zweiter Ansatz herangezogen.

Zusätzlich ist die Berücksichtigung der jeweiligen Bedrohungslage und möglicher Bedrohungsakteure sinnvoll, um sowohl die externen Faktoren als auch die aktuellen, sich dynamisch ändernden Bedrohungen angemessen zu berücksichtigen. Somit wird als dritter Ansatz die Bsedrohungs-basierte Herangehensweise des Risk Assessments bei der Entwicklung einer generischen Vorgehensweiseherangezogen. Insgesamt basiert die entwickelte generische Vorgehensweise damit auf drei Ansätzen, wodurch die unterschiedlichen Perspektiven sowie verschiedene Stärken kombiniert werden.

5.2 Relevante Aspekte im Hinblick auf kerntechnische Anlagen und Einrichtungen

Abschnitt 5.2 ist in der öffentlichen Version des Berichtes nicht enthalten.

5.3 Generische Vorgehensweise für deutsche kerntechnische Anlagen

Abschnitt 5.3 ist in der öffentlichen Version des Berichtes nicht enthalten.

6 Zusammenfassung und Fazit

Die Entwicklung einer generischen Vorgehensweise für die Durchführung eines Risk Assessments bzw. Risk Managements für schutzbedürftige IT-Systeme in kerntechnischen Anlagen und Einrichtungen steht im Zentrum dieses Vorhabens. Das Thema Risk Assessment bzw. Risk Management wird national und international vielfach in Normen und Leitlinien aufgegriffen, wobei das Thema unterschiedlich behandelt wird. Im Rahmen des Vorhabens wurde zunächst eine detaillierte Recherche in ausgewählten Regelwerken zu Anforderungen und Vorgehensweisen in Bezug auf Risk Assessment bzw. Risk Management Prozesse durchgeführt. Zudem wurde anhand es US-amerikanischen Beispiels eine länderspezifische Vorgehensweise betrachtet. Auf Basis der daraus gewonnenen Erkenntnisse wurde eine vergleichende Betrachtung zu unterschiedlichen Ansätzen, Herangehensweisen und Blickrichtungen für Risk Assessment Prozesse durchgeführt. Hierbei wurden mit dem Konsequenz-basierten, dem System-basierten, dem Bedrohungs-basierten und dem Schwachstellen-basierten Ansatz vier grundlegend unterschiedliche Ansätze für Risikobetrachtungen herausgearbeitet. Insbesondere wurden die einzelnen Schritte im Rahmen des Risk Assessments spezifisch für die unterschiedlichen Ansätze beschrieben und anschließend hinsichtlich ihrer Unterschiede in der Herangehensweise sowie der Vor- und Nachteile der einzelnen Ansätze diskutiert. Auf Basis dieser Diskussion wurden für die weiteren Arbeiten zur Entwicklung einer generischen Vorgehensweise für die Durchführung eines Risk Assessments in deutschen kerntechnischen Anlagen und Einrichtungen zunächst der Bedrohungs-basierte, der Konsequenz-basierte und der System-basierte Ansatz ausgewählt. Das Risk Assessment insgesamt stellt nach der Kontextualisierung von Risiken einen Schritt im Risk Management Prozess dar, an den sich der Schritt der Risiko-Behandlung anschließt, in dem der weitere Umgang mit den Risiken geplant wird. Zur Entwicklung einer generischen Vorgehensweise ist daher die Betrachtung des gesamten Risk Management Prozesses wesentlich. Daher enthalten die hier entwickelten Prozesse jeweils die fünf Schritte Risiko-Kontextualisierung, Riskio-Identifizierung, Risiko-Analyse, Risiko-Evaluierung und Risiko-Behandlung, welche den Risk Management Prozess ganzheitlich abbilden. Im Rahmen der Vorhabensbearbeitung wurde deutlich, dass im Rahmen der Entwicklung einer generischen Vorgehensweise für deutsche kerntechnische Anlage ein einzelner Ansatz für Risikobetrachtungen nicht ausreichend ist, da keiner der Ansätze allein in der Lage ist, die relevanten Aspekte abzudecken oder alle Vorgaben aus dem kerntechnischen Regelwerk zu erfüllen. Daher wurden die drei zuvor ausgewählten Ansätze im Rahmen der entwickelten Prozesse kombiniert.

Als weitere Erkenntnis ergab sich, dass die Prozessschritte bei einer erstmaligen Durchführung des Risk Management Prozesses von den Prozessschritten bei einer regelmäßigen oder anlassbezogenen Wiederholung des Risk Managements abweichen. Daher wurden für die erstmalige Durchführung, für die regelmäßige Durchführung und für die anlassbezogene Wiederholung jeweils eigenständige Prozesse entwickelt. Bei der anlassbezogenen Wiederholung wurde zudem unterschieden, ob die anlassbezogene Wiederholung des Risk Management Prozesses aufgrund von Änderungen hinsichtlich der IT-Bedrohungslage, aufgrund von Änderungen an IT-Systemen oder aufgrund von Änderungen bei der Einschätzung von unerwünschten Konsequenzen erfolgt. Zusätzlich wurde mittels des schwachstellen-basierten Ansatzes ein Risk Management Prozess für das Schwachstellenmanagement erarbeitet. Bei der Entwicklung dieser Prozesse standen zunächst Kernkraftwerke im Fokus. Anschließend wurde die Notwendigkeit von Anpassungen bei der Übertragung der Prozessschritte auf Zwischenlager und Anlagen der SK III diskutiert. Aufgrund des generischen Charakters der entwickelten Prozesse sowie der vergleichbaren Vorgaben aus dem kerntechnischen Regelwerk lassen sich die entwickelten Prozesse für alle kerntechnischen Anlagen, Einrichtungen und Tätigkeiten anwenden.

Literaturverzeichnis

/ATG21n01/ Gesetzentwurf der Bundesregierung, Entwurf eines Siebzehnten Gesetzes zur Änderung des Atomgesetzes (Siebzehntes AtG – ÄnderungsG), 11.01.2021

/ATG22n01/ Gesetz über die friedliche Verwendung der Kernenergie und den Schutz gegen ihre Gefahren (Atomgesetz), Fassung der Bekanntmachung vom 15. Juli 1985 (BGBl. I S. 1565), zuletzt geändert durch Artikel 1 des Gesetzes vom 4. Dezember 2022 (BGBl. I S. 2153)

/BMU13n01/ Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit, Interpretationen zu den Sicherheitsanforderungen an Kernkraftwerke, November 2013

/BMU13n03/ BMU, Richtlinie für den Schutz von IT-Systemen in kerntechnischen Anlagen und Einrichtungen der Sicherungskategorien I und II gegen Störmaßnahmen und sonstige Einwirkungen Dritter (SEWD-Richtlinie IT)

/BMU13n04/ BMU, Lastannahmen zur Auslegung kerntechnischer Anlagen und Einrichtungen gegen Störmaßnahmen oder sonstige Einwirkungen Dritter mittels IT-Angriffen (IT-Lastannahmen), VS-Vertraulich, 08.07.2013

/BMU13n05/ BMU, Erläuterungen für die Zuordnung der IT-Systeme von Kernkraftwerken zu IT-Schutzbedarfsklassen, VS-Vertraulich, 08.07.2013

/BMU13n06/ BMU, Bekanntmachung zur SEWD-Richtlinie IT, zu den IT-Lastannahmen und zu den Erläuterungen, RS-Handbuch, 3-99.1, 08.07.2013

/BMU15n01/ Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit, Sicherheitsanforderungen an Kernkraftwerke, November 2012, Neufassung vom 3. März 2015

/BMU17n01/ BMU, Erläuterungen für die Zuordnung der IT-Systeme von Zwischenlagern zu IT-Schutzbedarfsklassen, VS-Vertraulich, 23.06.2017

/BMU20n01/ BMU, Richtlinie für den Schutz von IT-Systemen in kerntechnischen Anlagen und bei Tätigkeiten der Sicherungskategorie III sowie der umsichtigen Betriebsführung gegen Störmaßnahmen und sonstige Einwirkungen Dritter (SEWD-Richtlinie IT SK III)

/BSI17n02/ Bundesamt für Sicherheit in der Informationstechnik, BSI-Standard 200-3, Risikoanalyse auf der Basis von IT-Grundschutz, Version 1.0, 2017

/BSI21r02/ Bundesamt für Sicherheit in der Informationstechnik, Die Lage der IT-Sicherheit in Deutschland 2021, September 2021

/CIS21b01/ Certified Information Systems Security Professional (CISSP), Mike Chapple, James Michael Stewart, Darril Gibson, 2021

/DIN19n01/ DIN, DIN EN 61511-1, Funktionale Sicherheit - PLT-Sicherheitseinrichtungen fuer die Prozessindustrie - Teil 1 (IEC 61511-1:2016), Deutsche Fassung EN 61511-1:2017, 2019

/DIN20n01/ DIN, DIN IEC 62645, Kernkraftwerke - Leittechische und elektrische Systeme - Anforderungen an die Cybersicherheit (IEC 62645:2019); Deutsche Fassung EN IEC 62645:2020, Oktober 2020

/GRS21r16/ Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) gGmbH, GRS-Bericht 647, "IT-Bedrohungslage in Bezug auf industrielle Steuerungssysteme und kritische Infrastrukturen - Stand Mai 2021"

/GRS23r02/ Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) gGmbH, GRS-Bericht 718, "IT-Bedrohungslage in Bezug auf industrielle Steuerungssysteme und kritische Infrastrukturen - Stand September 2022", November 2022

/GRS24r02/ Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) gGmbH, GRS-Bericht 757, IT-Bedrohungslage in Bezug auf industrielle Steuerungssysteme und kritische Infrastrukturen - Stand Februar 2024

/IAE18n02/ IAEA, IAEA Nuclear Security Series, Computer Security of Instrumentation and Control Systems at Nuclear Facilities, NSS 33-T, 2018

/IAE20n01/ IAEA, Nuclear Energy Series No. NR T 3.30, Nuclear Energy Series No. NR T 3.30, 2020

/IAE21n01/ IAEA, IAEA Nuclear Security Series, Implementation Guide, Computer Security for Nuclear Security , NSS 42-G, 2021

/IAE21n02/ IAEA, IAEA Nuclear Security Series, Computer Security Techniques for Nuclear Facilities, NSS 17-T, Rev.1, 2021

/IEC09n03/ IEC, IEC TS 62443-1-1:2009, Industrial communication networks - Network and system security - Part 1-1: Terminology, concepts and models, 2009

/IEC19n04/ IEC, IEC 31010, Risk management - Risk assessment techniques, 2019

/ISO17n02/ DIN EN ISO/IEC27001, Informationstechnik Sicherheitsverfahren InformationssicherheitsmanagementsystemeAnforderungen(ISO/IEC 27001:2013 einschließlich Cor1:2014 und Cor2:2015), Deutsche Fassung ENISO/IEC27001:2017, Juni 2017

/ISO17n03/ DIN EN ISO/IEC27002, Informationstechnik - Sicherheitsverfahren - LeitfadenfürInformationssicherheitsmaßnahmen(ISO/IEC27002:2013 einschließlich Cor1:2014 und Cor2:2015), Deutsche Fassung EN ISO/IEC 27002:2017, Juni 2017

/ISO18n03/ ISO, International Standard ISO/IEC 27005, Information technology security techniques Information security risk management, 2018

/ISO18n04/ DIN ISO 31000, Risikomanagement - Leitlinien (ISO 31000:2018), Deutsche Fassung ISO 31000:2018, 2018

/ISO21n01/ ISO/SAE 21434:2021, Road vehicles - Cybersecurity engineering, August 2021

/ISO22n01/ ISO/IEC 18045:2022, Information security, cybersecurity and privacy protection - Evaluation criteria for IT security - Methodology for IT security evaluation, August 2022

/NIS11n01/ NIST Special Publication 800-39, Managing Information Security Risk, 2011

/NIS12n01/ National Institute of Standards and Technology, NIST Special Publication 800-30, Revision 1, Information Security, Guide for Conducting Risk Assessments, September 2012

/NIS18n01/ NIST SP 800-37 Rev. 2 Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy, 2018

/NIS20r01/ NIST, SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations, September 2020

/NIS24n01/ NIST, The NIST cybersecurity framework (CSF) 2.0, February 2024

Abbildungsverzeichnis

Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) gGmbH

Schwertnergasse 1
50667 Köln
Telefon +49 221 2068-0
Telefax +49 221 2068-888

Boltzmannstraße 14
85748 Garching b. München
Telefon +49 89 32004-0
Telefax +49 89 32004-300

Kurfürstendamm 200
10719 Berlin
Telefon +49 30 88589-0
Telefax +49 30 88589-111

Theodor-Heuss-Straße 4
38122 Braunschweig
Telefon +49 531 8012-0
Telefax +49 531 8012-200

www.grs.de

ISBN 978-3-911727-12-9