

DIN EN 18037

ICS 35.030

Einsprüche bis 2024-01-17

Entwurf**Leitlinien für ein sektorales Cybersecurity Assessment;
Deutsche und Englische Fassung prEN 18037:2023**

Guidelines on a sectoral cybersecurity assessment;
German and English version prEN 18037:2023

Lignes directrices pour une évaluation sectorielle de la cybersécurité;
Version allemande et anglaise prEN 18037:2023

Anwendungswarnvermerk

Dieser Entwurf mit Erscheinungsdatum 2023-11-17 wird der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt.

Weil das beabsichtigte Dokument von der vorliegenden Fassung abweichen kann, ist die Anwendung dieses Entwurfs besonders zu vereinbaren.

Stellungnahmen werden erbeten

- vorzugsweise online im Norm-Entwurfs-Portal von DIN unter www.din.de/go/entwuerfe bzw. für Norm-Entwürfe der DKE auch im Norm-Entwurfs-Portal der DKE unter www.entwuerfe.normenbibliothek.de, sofern dort wiedergegeben;
- oder als Datei per E-Mail an nia@din.de möglichst in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter www.din.de/go/stellungnahmen-norm-entwuerfe oder für Stellungnahmen zu Norm-Entwürfen der DKE unter www.dke.de/stellungnahme abgerufen werden;
- oder in Papierform an den DIN-Normenausschuss Informationstechnik und Anwendungen (NIA), 10772 Berlin oder Am DIN-Platz, Burggrafenstr. 6, 10787 Berlin.

Es wird gebeten, mit den Kommentaren zu diesem Entwurf jegliche relevanten Patentrechte, die bekannt sind, mitzuteilen und unterstützende Dokumentationen zur Verfügung zu stellen.

Gesamtumfang 136 Seiten

DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)

Nationales Vorwort

Dieses Dokument (prEN 18037:2023) wurde vom Technischen Komitee CEN/CLC/JTC 13 „Cybersicherheit und Datenschutz“ erarbeitet, dessen Sekretariat von DIN (Deutschland) gehalten wird.

Das zuständige nationale Normungsgremium ist der Gemeinschaftsarbeitsausschuss NA 043-04-13 GA „DIN/DKE Gemeinschaftsgremium Cybersecurity“ im DIN-Normenausschuss Informationstechnik und Anwendungen (NIA).

Um Zweifelsfälle in der Übersetzung auszuschließen, ist die englische Originalfassung beigelegt. Die Nutzungsbedingungen für den deutschen Text des Norm-Entwurfes gelten gleichermaßen auch für den englischen Text.

Für die in diesem Dokument zitierten Dokumente wird im Folgenden auf die entsprechenden deutschen Dokumente hingewiesen:

ISO 31000	siehe	DIN ISO 31000
ISO/IEC 15408-1 (alle Teile)	siehe	DIN EN ISO/IEC 15408-1 (alle Teile)
ISO/IEC 18045	siehe	DIN EN ISO/IEC 18045
ISO/IEC 27001	siehe	DIN EN ISO/IEC 27001
ISO/IEC 27002	siehe	DIN EN ISO/IEC 27002
ISO/IEC 27011	siehe	DIN EN ISO/IEC 27011
ISO/IEC 27019	siehe	DIN EN ISO/IEC 27019

Aktuelle Informationen zu diesem Dokument können über die Internetseiten von DIN (www.din.de) durch eine Suche nach der Dokumentennummer aufgerufen werden.

Nationaler Anhang NA (informativ)

Literaturhinweise

DIN EN ISO/IEC 15408-1 (alle Teile), *Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre — Evaluationskriterien für IT-Sicherheit*

DIN EN ISO/IEC 18045, *Informationstechnik — Sicherheitstechniken — Methodik für die Bewertung der IT-Sicherheit*

DIN EN ISO/IEC 27001, *Informationstechnik — Sicherheitsverfahren — Informationssicherheitsmanagementsysteme — Anforderungen*

DIN EN ISO/IEC 27002, *Informationstechnik — Sicherheitsverfahren — Leitfaden für Informationssicherheitsmaßnahmen*

DIN EN ISO/IEC 27011, *Informationstechnik — Sicherheitsverfahren — Leitfaden für Informationssicherheitsmaßnahmen auf Grundlage von ISO/IEC 27002 für Telekommunikationsorganisationen*

DIN EN ISO/IEC 27019, *Informationstechnik — Sicherheitsverfahren — Informationssicherheitsmaßnahmen für die Energieversorgung*

DIN ISO 31000, *Risikomanagement — Leitlinien*

– *Entwurf* –

E DIN EN 18037:2023-12

– Leerseite –

November 2023

prEN 18037

Leitlinien für ein sektorales Cybersecurity Assessment

Guidelines on a sectoral cybersecurity assessment

Lignes directrices pour une évaluation sectorielle de la cybersécurité

Inhalt

	Seite
Europäisches Vorwort	5
Einleitung	6
1 Anwendungsbereich	8
2 Normative Verweisungen	8
3 Begriffe	8
3.1 Allgemeine Begriffe	8
3.2 Begriffe im Zusammenhang mit Organisation	9
3.3 Begriffe im Zusammenhang mit einem sektoralen Cybersicherheitsansatz	10
3.4 Begriffe im Zusammenhang mit Risiko	11
4 Abkürzungen	13
5 Sektorales Cybersecurity Assessment	13
5.1 Anwendung der Methodik für sektorale Cybersecurity Assessments	13
5.2 Grundsätze und neue Potentiale	15
6 Sektorale Darstellung von Risiken	18
6.1 Sektorale IKT-Systeme	18
6.1.1 Sektorale IKT-Systemkomponenten und ihre Beziehungen	18
6.1.2 Mehrschichtige Architektur sektoraler IKT-Systeme	18
6.1.3 Risikobasierte Definitionen von Cybersecurity- und Vertrauenswürdigkeitsanforderungen in sektoralen Systemen	21
6.1.4 Relevanz der sektoralen IKT-Systemarchitektur für die Risikobewertung	21
6.1.5 Cybersecurity-Zertifizierung sektoraler IKT-Systeme	22
6.2 Einheitliche sektorale Risikobewertung	23
6.3 Durchführung einer sektoralen Risikobewertung	24
6.3.1 Allgemeines	24
6.3.2 Wahl des Ansatzes	25
6.3.3 Identifizierung von Geschäftsprozessen, -zielen und -anforderungen	25
6.3.4 Identifizierung von Primärwerten und unterstützenden Werten	25
6.3.5 Definition von Risikoszenarien	26
6.3.6 Bewertung der Folgen in Risikoszenarien	26
6.3.7 Bewertung der Wahrscheinlichkeit in Risikoszenarien	27
6.3.8 Integration der Angreiferperspektive: Bewertung des Angriffspotentials	28
6.3.9 Erneute Risikobewertung für unterstützende Werte	29
7 Normalisierte Darstellung von Risiko, Cybersecurity und Vertrauenswürdigkeit	30
7.1 Ergebnisse von Risikobewertungen: Meta-Risikoklassen	30
7.2 Risikobasierte Definition von allgemeinen Sicherheitsstufen und Auswahl von Sicherheitsmaßnahmen	30
7.2.1 Allgemeines	30
7.2.2 Einführung von allgemeinen Sicherheitsstufen (CSL)	31
7.2.3 Einsatz von Meta-Risikoklassen und allgemeinen Sicherheitsstufen zur sektoralen Risikobehandlung	31
7.2.4 Angriffspotential als Kriterium für die Auswahl der CSL von Maßnahmen	31
7.3 Einheitliche Implementierung von Vertrauenswürdigkeit	32
7.3.1 Einführung	32
7.3.2 Definition eines allgemeinen Vertrauenswürdigkeitsreferenzkonzepts basierend auf ISO/IEC 15408	32
7.3.3 Anwendung des CTI-Konzepts zum Angriffspotential auf CAR	33
8 Zuordnung von Cybersecurity- und Vertrauenswürdigkeitsanforderungen zur Programmdarstellung	34
Anhang A (informativ) Beispiele für normalisierte Skalen bei der sektoralen Risikobewertung	35
A.1 Qualitativer Ansatz zur Bewertung der Folgen	35
A.2 Qualitativer Ansatz zur Wahrscheinlichkeitsbewertung	37

A.3	Qualitativer Ansatz zur Risikoeinschätzung	37
A.4	Qualitativer Ansatz zur Risikominderung	38
A.5	Meta-Risikoklassen durch eine Klassifizierung der allgemeinen Vertrauenswürdigkeitsreferenz adressieren	38
Anhang B (informativ)	CTI-Grundlagen	40
B.1	Allgemeines	40
B.2	Angreifertypen	41
B.3	Merkmale der Angreifer	42
B.4	Kriterien für eine qualitative Einschätzung des Angriffspotentials	46
B.4.1	Merkmale: Gelegenheit	46
B.4.2	Merkmale: Mittel	50
B.4.3	Merkmal: Motive	53
B.5	Einschätzung des Angriffspotentials mithilfe des CTI-Ansatzes	56
B.5.1	Allgemeines	56
B.5.2	Merkmale: Gelegenheit	56
B.5.3	Merkmale: Mittel	57
B.5.4	Merkmale: Motive	58
B.5.5	Berechnung des Angriffspotentials (APL)	58
B.5.6	Eine Gleichwertigkeit zwischen CTI und ISO/IEC 18045 für die Einschätzung des Angriffspotentials finden	59
Anhang C (informativ)	Anwendung des Ansatzes der allgemeinen Sicherheitsstufen — Beispiele	62
C.1	Allgemeines	62
C.2	Anwendungsbeispiel: Mobilgerät-basiertes Authentifizierungssystem	62
C.3	Anwendungsbeispiel: Schutz gegen geklonte Geräte und betrügerische Anbieter	65
Anhang D (informativ)	Beispiel für die Zuordnung einer Vertrauenswürdigkeitsstufe	67
Literaturhinweise		68

Bilder

Bild 1	Sektorales Cybersecurity Assessment	14
Bild 2	Überblick über die vom sektoralen Cybersecurity Assessment genutzten und generierten Informationen	16
Bild 3	Beziehung zwischen IKT-Dienstleistungen, IKT-Produkten und IKT-Prozessen	18
Bild 4	Schichten eines sektoralen IKT-Systems	20
Bild 5	Beziehung zwischen Geschäftsprozessen, Primärwerten und unterstützenden Werten	22
Bild 6	Sektorale Risikobewertung	25
Bild B.1	Merkmale des Angreifers	40
Bild B.2	Komponente zur Einschätzung des Angriffspotentials	43

Tabellen

Tabelle 1	Zuordnung der allgemeinen Vertrauenswürdigkeitsreferenz (CAR)	33
Tabelle A.1	Wirkungsklassen — Beispiel 1	35
Tabelle A.2	Wirkungsklassen je Risikobereich — Beispiel 2	36
Tabelle A.3	Wahrscheinlichkeitsbewertung — ein Beispiel	37
Tabelle A.4	Meta-Risikoklassen — Beispiel	37
Tabelle A.5	Allgemeine Sicherheitsstufen — Beziehungen zu Meta-Risikoklassen und Angriffspotentials	38
Tabelle A.6	Kombinationen von MRC, AP und CAR — Beispiel	39
Tabelle B.1	Beschreibung des Angriffspotentials anhand von Systemzugriff und -wissen	43
Tabelle B.2	Beschreibung des Angriffspotentials anhand von Schwachstellen	43
Tabelle B.3	Beschreibung des Angriffspotentials in Abwesenheit bekannter Schwachstellen	44
Tabelle B.4	Beschreibung des Angriffspotentials anhand von Fähigkeiten und Ressourcen	44

Tabelle B.5 — Beschreibung des Angriffspotentials anhand von Fähigkeitsmerkmalen	45
Tabelle B.6 — Beschreibung des Angriffspotentials anhand der Wertwahrnehmung	45
Tabelle B.7 — Beschreibung des Angriffspotentials anhand von Zielen	45
Tabelle B.8 — Qualitativer Angriffswert nach Zugang/Zeit mit dem unterstützenden Wert zur Angriffsvorbereitung	46
Tabelle B.9 — Qualitativer Angriffswert nach Zugang/Zeit mit dem unterstützenden Wert zur Angriffsdurchführung	47
Tabelle B.10 — Qualitativer Angriffswert nach Wissen über den unterstützenden Wert	47
Tabelle B.11 — Qualitativer Angriffswert nach Wissen über die Schwachstellen	48
Tabelle B.12 — Qualitativer Angriffswert nach Zugang zur Quelle des unterstützenden Werts . .	48
Tabelle B.13 — Qualitativer Angriffswert nach Fähigkeit, auf unterstützende Werte in der Lieferkette zuzugreifen/diese zu modifizieren	49
Tabelle B.14 — Qualitativer Angriffswert nach Fähigkeit zum Anwerben von Insidern	49
Tabelle B.15 — Qualitativer Angriffswert nach Art der vom Angreifer genutzten Ausstattung . .	50
Tabelle B.16 — Qualitativer Angriffswert nach Vermeidung von Sichtbarkeit	51
Tabelle B.17 — Qualitativer Angriffswert nach Mitteln zum Ersatz fehlender Komponenten . . .	52
Tabelle B.18 — Qualitativer Angriffswert nach allgemeinem Angriffswissen	52
Tabelle B.19 — Qualitativer Angriffswert nach Verfügbarkeit der Angriffsmethode	53
Tabelle B.20 — Qualitativer Angriffswert nach Zeitfenster zum Erreichen der Ziele	54
Tabelle B.21 — Qualitativer Angriffswert nach dem für den Angreifer daraus abgeleiteten Wert .	54
Tabelle B.22 — Qualitativer Angriffswert nach Zielsetzung	55
Tabelle B.23 — Qualitativer Angriffswert nach rechtlichen und ethischen Beschränkungen . . .	55
Tabelle B.24 — Qualitativer Angriffswert nach geopolitischem Kontext	56
Tabelle B.25 — Zusammenfassung der CTI-Kriterien zur Anwendung in der APL-Bewertung . . .	59
Tabelle B.26 — Methode zur Einschätzung des APL durch Anwendung der für die Anfälligkeitsanalyse relevanten CTI-Merkmale	60
Tabelle C.1 — Anwendungsbeispiel des CSL-Ansatzes — CSL2	63
Tabelle C.2 — Anwendungsbeispiel des CSL-Ansatzes — CSL3	64
Tabelle C.3 — Anwendungsbeispiel des CSL-Ansatzes — CSL4	65
Tabelle C.4 — Anwendungsbeispiel eines CSL-Ansatzes mit mehreren Sicherheitsebenen	66

Europäisches Vorwort

Dieses Dokument (prEN 18037:2023) wurde vom Technischen Komitee CEN/CLC/JTC 13 „Cybersicherheit und Datenschutz“ erarbeitet, dessen Sekretariat von DIN gehalten wird.

Dieses Dokument ist derzeit zur CEN-Umfrage vorgelegt.

Einleitung

Dieses Dokument beschreibt Cybersecurity Assessments auf Marktsektor- oder Anwendungsebene. Es soll als Vorbereitung für den Entwurf von Cybersecurity-Zertifizierungsprogrammen für IKT-Produkte, IKT-Prozesse und IKT-Systeme genutzt werden, die einem Marktsektor zur Bereitstellung sektoraler Dienstleistungen an Endnutzer oder Geschäftskunden dienen, wobei somit sektorale IKT-Systeme gebildet werden.

Sektorale IKT-Systeme finden sich in Anwendungsbereichen wie Mobilfunknetzen, digitalen Identitätsdiensten, E-Health, öffentlichen Verkehrsmitteln oder Zahlungssystemen.

Sektorale IKT-Systeme können eine große Anzahl von Stakeholder-Organisationen aus dem gleichen Marktsektor einbeziehen, die in festgelegten Rollen an der Bereitstellung sektoraler Dienstleistungen mitwirken. Bei bestimmten Rollen, beispielsweise bei Mobilfunknetzbetreibern oder öffentlichen Verkehrsdienstleistern, stehen die Stakeholder-Organisationen möglicherweise im Wettbewerb zueinander.

Die an einem sektoralen IKT-System beteiligten Stakeholder-Organisationen agieren entsprechend bestimmter Regeln, die üblicherweise von einer „koordinierenden Einheit“ oder Regulierungsbehörde definiert werden, und betreiben die von ihnen kontrollierten IKT-Systeme oder -Produkte als Funktionskomponenten des sektoralen IKT-Systems.

Cybersecurity und Vertrauenswürdigkeit sind jedoch nicht nur aus Sicht der Kunden sektoraler Dienstleistungen relevant. Im sektoralen IKT-System ist es wichtig, klare und einheitliche Cybersecurity- und Vertrauenswürdigkeitsanforderungen im Hinblick auf die Stakeholder-Rolle zu definieren, um für Vertrauen unter den sektoralen Stakeholder-Organisationen zu sorgen. Denn durch einen Stakeholder verursachte IKT-Sicherheitsmängel können die Geschäftsziele anderer Stakeholder gefährden.

Wie bei jedem IKT-System, das erhöhte Cybersecurity- und Vertrauenswürdigkeitsanforderungen erfüllen soll, müssen die sektoralen Stakeholder-Organisationen das richtige Gleichgewicht zwischen der Notwendigkeit von Cybersecurity und Vertrauenswürdigkeit und den damit verbundenen Implementierungskosten finden. Im Hinblick auf die Definition von Cybersecurity- und Zertifizierungsanforderungen an das sektorale IKT-System sollen diese durch die Identifizierung der Risiken für die Geschäftsziele der Stakeholder und das Angriffspotential relevanter Angreifertypen im Zusammenhang mit der bestimmungsgemäßen Nutzung gestützt werden.

Ein sektorales IKT-System unterstützt eine Vielzahl von Geschäftsprozessen und Geschäftszielen der Stakeholder, die allesamt Cybersicherheitsrisiken ausgesetzt sein können. Es kann auch ein breites Spektrum an von Stakeholdern betriebenen IKT-Systemen, -Produkten und -Prozessen beinhalten, die zur Validierung der Implementierung von Cybersecurity- und Vertrauenswürdigkeitsanforderungen meist unterschiedliche Evaluierungs- und Zertifizierungsansätze erfordern. Vertrauenswürdige sektorale Dienstleistungen setzen Vertrauen zwischen den sektoralen Stakeholdern voraus. Dies gilt auch für die Wiederverwendung von Zertifikaten. Zertifizierte Komponenten erfordern eine Definition von Vertrauenswürdigkeit und Cybersecurity, die für Konsistenz sorgt. Dafür stellt die Spezifizierung von Anforderungen und die Definition von Risikoniveaus zur Evaluierung und Zertifizierung die Basis dar.

Die Methodik für sektorale Cybersecurity Assessments unterstützt die Aspekte und Anforderungen durch die folgenden Merkmale:

- Das sektorale Cybersecurity Assessment wird Informationen zu den vom sektoralen IKT-System zu unterstützenden Geschäftsprozessen sowie den dazugehörigen Geschäftszielen der sektoralen Stakeholder bereitstellen. Zudem identifiziert es die primären und unterstützenden Werte, die für eine sichere Implementierung der Geschäftsprozesse entscheidend sind (siehe 5.2 und 6.3.3).
- Die von den Stakeholdern betriebenen IKT-Systeme oder -Prozesse, die für die Sicherheit der Primärwerte relevant sind, werden identifiziert. Eine Vertiefung in die Architektur des sektoralen IKT-Systems bietet detaillierte Informationen über seine bestimmungsgemäße Nutzung (siehe 6.1).
- Cyber Threat Intelligence Information (CTI), also sicherheitsrelevante Informationen zu bestehenden Cyberbedrohungen, werden dazu genutzt, Informationen über möglicherweise relevante Angreifertypen,

ihre Motivation und ihre Fähigkeiten zu sammeln. CTI ermöglicht es, diejenigen Risikoszenarien zu priorisieren, die für eine weitere Analyse am relevantesten sind. Dies erlaubt die effektivste Nutzung der zur Analyse benötigten Ressourcen und trägt dazu bei, die für die Zuordnung der Cybersecurity- und Vertrauenswürdigkeitsanforderungen zu IKT-Systemen, IKT-Produkten oder IKT-Dienstleistungen erforderlichen Informationen basierend auf dem mit der bestimmungsgemäßen Nutzung verbundenen Risiko bereitzustellen (siehe 6.3.8 und Anhang B).

- Cybersicherheitsrisiken werden anhand der Folgen von Cybersicherheitsvorfällen für die Geschäftsziele der Stakeholder sowie der Wahrscheinlichkeit ihres Auftretens identifiziert und bewertet (siehe 6.3.6 beziehungsweise 6.3.7). Die Bewertung der Wahrscheinlichkeit leitet sich aus der möglichen Motivation derjenigen Angreifertypen ab, die in der Lage sind, Angriffe auf die identifizierten Werte durchzuführen.
- Die Methodik bietet ein Konzept mit Referenzwerten zu internen Risiken, Cybersecurity, Vertrauenswürdigkeit und Angriffspotential (siehe Abschnitt 7). Allgemein angewendet unterstützen sie eine einheitliche Definition von Risiko, Cybersecurity und Vertrauenswürdigkeit. Die Methodik bietet die Möglichkeit, sektoral-, produkt-, prozess- und möglicherweise auch ISMS-basierte Cybersecurity-Zertifizierungsprogramme zu integrieren und kann IKT-Produktzertifizierungsprogramme über Common Criteria oder andere ISO/IEC 15408-basierte Programme hinaus unterstützen und integrieren.
- Die durch einen ISO/IEC 27005-konformen Ansatz auf Sektorebene erhaltenen Risikoinformationen können auf ISO/IEC 15408-basierte Umgebungen übertragen werden. Durch die Anwendung von zwei verschiedenen Standards kann die risikobasierte Definition von Cybersecurity- und Vertrauenswürdigkeitsanforderungen unterstützt werden (siehe 5.2 und Abschnitt 8).

Basierend auf diesen Eigenschaften und Funktionen profitieren die sektoralen Stakeholder auf folgende Weise:

- Die Methodik unterstützt die Identifizierung von mit der Nutzung von IKT-Systemen, IKT-Dienstleistungen und IKT-Prozessen verbundenen Risiken auf jeder Ebene der sektoralen IKT-Systemarchitektur. Die sektoralen Stakeholder-Organisationen können ihre Risikoeinschätzung gegen die zur Risikominderung erforderlichen Investitionen abwägen, indem sie angemessene Sicherheits- und Vertrauenswürdigkeitsstufen einführen. Es kann erwartet werden, dass dieser transparente, kooperative Ansatz signifikant zur Marktakzeptanz dieser Anforderungen und der darauf basierenden Cybersecurity-Zertifizierungsprogramme beitragen wird.
- Es kann eine programmübergreifende Konsistenz bei der Implementierung der Vertrauenswürdigkeitsstufen erzielt werden. Auf diese Weise wird eine Wiederverwendung der von einem Programm ausgestellten Zertifikate in anderen Programmen ermöglicht, was einen wichtigen Vorteil für die Geschäftsinteressen der Produkt- und Infrastrukturdienstleister sowie für deren Kunden darstellt. Gleichzeitig ist der von der Methodik vorgeschlagene Ansatz für mehr Konsistenz flexibel genug, um die Integration neuer Arten von Cybersecurity-Zertifizierungsprogrammen zu unterstützen, die aufgrund spezieller Anforderungen unterschiedlicher Märkte auftreten können.
- Einführung eines allgemeinen Konzepts für Sicherheitsstufen, das die Definition von Sicherheitsmaßnahmen, die programmübergreifend zur Cybersecurity-Zertifizierung genutzt werden können, erleichtert.

Zusammenfassend unterstützt die vorgeschlagene Methodik nicht nur den Workflow für den Entwurf marktorientierter Cybersecurity-Zertifizierungsprogramme, sondern bietet auch das Potential für eine breitere Anwendung durch Sektoren und Infrastrukturanbieter.

1 Anwendungsbereich

Dieses Dokument legt einen Ansatz, der eine risikobasierte Identifizierung von Cybersecurity-, Zertifizierungs- und Vertrauenswürdigkeitsanforderungen von IKT-Produkten, -Prozessen und -Dienstleistungen für komplexe, sektorale Multi-Stakeholder-Systeme unterstützt, fest.

Der sektorale Cybersecurity-Assessment-Prozess beinhaltet alle zur Definition, Implementierung und Aufrechterhaltung dieser Anforderungen erforderlichen Schritte.

2 Normative Verweisungen

Die folgenden Dokumente werden im Text in solcher Weise in Bezug genommen, dass einige Teile davon oder ihr gesamter Inhalt Anforderungen des vorliegenden Dokuments darstellen. Bei datierten Verweisungen gilt nur die in Bezug genommene Ausgabe. Bei undatierten Verweisungen gilt die letzte Ausgabe des in Bezug genommenen Dokuments (einschließlich aller Änderungen).

ISO/IEC 15408, *Information security, cybersecurity and privacy protection — Evaluation criteria for IT security*

ISO/IEC 27005, *Information security, cybersecurity and privacy protection — Guidance on managing information security risks*

3 Begriffe

Für die Anwendung dieses Dokuments gelten die folgenden Begriffe.

ISO und IEC stellen terminologische Datenbanken für die Verwendung in der Normung unter den folgenden Adressen bereit:

- IEC Electropedia: verfügbar unter <https://www.electropedia.org/>
- ISO Online Browsing Platform: verfügbar unter <https://www.iso.org/obp>

3.1 Allgemeine Begriffe

3.1.1

Informationssicherheit

Bewahrung der Vertraulichkeit, Integrität und Verfügbarkeit von Information

[QUELLE: EN ISO/IEC 27000:2018, 3.28]

3.1.2

Cybersicherheit

Cybersecurity

Schutz von Menschen, Gesellschaften, Organisationen und Ländern vor Cyberrisiken (*Risiko* [3.4.1])

Anmerkung 1 zum Begriff: Schutz bedeutet, Cyberrisiken (*Risiko*, 3.4.1) auf einem tolerierbaren Niveau zu halten.

[QUELLE: ISO/IEC 27100, 3.2]

3.1.3

Vertrauenswürdigkeitsstufe

Grundlage für das Vertrauen, dass ein *IKT-Produkt* (3.3.4), eine *IKT-Dienstleistung* (3.3.5) oder ein *IKT-Prozess* (3.3.6) den Cybersicherheitsanforderungen (*Anforderung* [3.2.5]) entspricht

Anmerkung 1 zum Begriff: Cybersicherheitsanforderungen (*Anforderung* [3.2.5]) können in einem Cybersecurity-Zertifizierungsprogramm festgeschrieben werden.

Anmerkung 2 zum Begriff: Eine Vertrauenswürdigkeitsstufe zeigt die Ebene an, auf der ein *IKT-Produkt* (3.3.4), eine *IKT-Dienstleistung* (3.3.5) oder ein *IKT-Prozess* (3.3.6) evaluiert wurde.

Anmerkung 3 zum Begriff: Vertrauenswürdigkeitsstufen bewerten nicht die Cybersicherheit des betreffenden *IKT-Produkts* (3.3.4), der betreffenden *IKT-Dienstleistung* (3.3.5) oder des betreffenden *IKT-Prozesses* (3.3.6) (vgl. [6], Artikel 2.22).

Anmerkung 4 zum Begriff: Dieser Standard nutzt die Beziehung zwischen Vertrauenswürdigkeitsstufen und der Widerstandsfähigkeit des Evaluierungsgegenstandes gegen bestimmte *Angriffspotentiale* (3.4.9), wie in ISO/IEC 15408-3 definiert, als Parameter für die Implementierung einheitlicher Vertrauenswürdigkeitsstufen im Rahmen von Cybersecurity-Zertifizierungsprogrammen sowie für die Identifizierung von potentiellen Vertrauenswürdigkeitsstufen in bestehenden Programmen.

3.2 Begriffe im Zusammenhang mit Organisation

3.2.1

Organisation

Person oder Personengruppe, die eigene Funktionen mit Verantwortlichkeiten, Befugnissen und Beziehungen hat, um ihre *Ziele* (3.3.2) zu erreichen

Anmerkung 1 zum Begriff: Der Begriff Organisation umfasst unter anderem Einzelunternehmer, Gesellschaft, Konzern, Firma, Unternehmen, Behörde, Handelsgesellschaft, Wohltätigkeitsorganisation, Institution, oder Teile oder eine Kombination der genannten, ob eingetragen oder nicht, öffentlich oder privat.

[QUELLE: EN ISO/IEC 27000:2018, 3.50]

3.2.2

Ziel

zu erreichendes Ergebnis

Anmerkung 1 zum Begriff: Ein Ziel kann strategisch, taktisch oder operativ sein.

Anmerkung 2 zum Begriff: Ziele können sich auf verschiedene Disziplinen beziehen (z. B. finanzielle, gesundheits- und sicherheitsbezogene sowie umweltbezogene Ziele) und für verschiedene Ebenen gelten (z. B. strategische, organisationsweite, Projekt, Produkt und Prozess).

[QUELLE: EN ISO/IEC 27000:2018, 3.49, modifiziert – Anmerkung 3 und Anmerkung 4 gelöscht]

3.2.3

Politik

Absichten und Ausrichtung einer *Organisation* (3.2.1), wie von der obersten Leitung formell ausgedrückt

[QUELLE: EN ISO/IEC 27000:2018, 3.53]

3.2.4

Prozess

Satz zusammenhängender und sich gegenseitig beeinflussender Tätigkeiten, der Eingaben in Ergebnisse umwandelt

[QUELLE: EN ISO/IEC 27000:2018, 3.54]

3.2.5

Anforderung

Erfordernis oder Erwartung, das oder die festgelegt, üblicherweise vorausgesetzt oder verpflichtend ist

Anmerkung 1 zum Begriff: „Üblicherweise vorausgesetzt“ bedeutet, dass es für die *Organisation* (3.2.1) und andere interessierte Parteien üblich oder allgemeine Praxis ist, dass das entsprechende Erfordernis oder die entsprechende Erwartung vorausgesetzt wird.

Anmerkung 2 zum Begriff: In ISO/IEC 15408 wird der Begriff „Anforderung“ in direktem Zusammenhang mit „Sicherheitszielsetzungen“ verwendet.

[QUELLE: EN ISO/IEC 27000:2018, 3.56, modifiziert – Anmerkung 2 zum Begriff gelöscht, neue Anmerkung 2 zum Begriff hinzugefügt]

3.3 Begriffe im Zusammenhang mit einem sektoralen Cybersicherheitsansatz

3.3.1

Sektor

Marktsektor

Bereich, in dem Geschäftsprozesse und Anwendungsfälle größtenteils unter denselben Randbedingungen implementiert werden können

Anmerkung 1 zum Begriff: „Marktsektor“ und „Anwendungsbereich“ können synonym verwendet werden.

Anmerkung 2 zum Begriff: Randbedingungen beinhalten die relevanten Stakeholder- und Kundentypen, die zu unterstützenden Dienstleistungen sowie rechtliche und kommerzielle Aspekte.

3.3.2

sektorales IKT-System

System, das die *IKT-Produkte* (3.3.4) und *IKT-Prozesse* (3.3.5) beinhaltet, die zur Bereitstellung der Dienstleistungen an die Nutzer eines bestimmten Marktsektors erforderlich sind

Anmerkung 1 zum Begriff: Sektorale IKT-Systeme können bei speziellen Funktionen auf IKT-Infrastrukturdienste angewiesen sein.

Anmerkung 2 zum Begriff: Immer, wenn für die Cybersicherheit relevante Funktionen eines sektoralen IKT-Systems auf externe IKT-Dienstleistungen angewiesen sind, werden diese als IKT-Infrastrukturdienste betrachtet.

Anmerkung 3 zum Begriff: Sektorale IKT-Systeme können von verschiedenen Stakeholdern betrieben werden.

3.3.3

sektorale IKT-Systemarchitektur

Spezifizierung einer koordinierten Nutzung mehrerer *sektoraler IKT-Systeme* (3.3.2), *IKT-Produkte* (3.3.4), *IKT-Prozesse* (3.3.5) und *IKT-Dienstleistungen* (3.3.6), die die Implementierung und den Betrieb von Sektordienstleistungen ermöglichen

Anmerkung 1 zum Begriff: Die drei folgenden Definitionen stammen aus [6].

3.3.4

IKT-Produkt

Element oder Gruppe von Elementen eines Netzwerk- oder Informationssystems

3.3.5

IKT-Prozess

Reihe von Aktivitäten, die zum Design, zur Entwicklung, zur Bereitstellung oder zur Aufrechterhaltung eines *IKT-Produkts* (3.3.4) oder einer *IKT-Dienstleistung* (3.3.6) durchgeführt werden

3.3.6

IKT-Dienstleistung

Dienstleistung, die vollumfänglich oder hauptsächlich aus der Übertragung, Speicherung, Abrufung oder Verarbeitung von Informationen mithilfe von Netzwerk- oder Informationssystemen besteht

3.4 Begriffe im Zusammenhang mit Risiko

3.4.1

Risiko

Auswirkung von Unsicherheit auf *Ziele* (3.2.2)

Anmerkung 1 zum Begriff: Eine Auswirkung stellt eine – positive oder negative – Abweichung vom Erwarteten dar.

Anmerkung 2 zum Begriff: *Ziele* (3.2.2) können verschiedene Aspekte und Kategorien umfassen und auf verschiedenen Ebenen angewendet werden.

Anmerkung 3 zum Begriff: Ungewissheit ist der Zustand des auch teilweisen Fehlens von Information im Hinblick auf das Verständnis eines Ereignisses oder Wissen über ein *Ereignis*, seine Folgen oder seine Wahrscheinlichkeit.

Anmerkung 4 zum Begriff: Das Risiko wird üblicherweise anhand der Risikoursachen, der potentiellen Ereignisse, ihrer Auswirkungen und ihrer Wahrscheinlichkeit dargestellt.

Anmerkung 5 zum Begriff: Im Kontext von Informationssicherheitsmanagementsystemen können Informationssicherheitsrisiken (*Informationssicherheit* [3.1.1]) als Auswirkung von Ungewissheit auf Informationssicherheitsziele (*Informationssicherheit* [3.1.1], *Ziel* [3.2.2]) beschrieben werden.

Anmerkung 6 zum Begriff: Informationssicherheitsrisiken (*Informationssicherheit* [3.1.1]) sind stets mit einer negativen Auswirkung von Ungewissheit auf *Informationssicherheitsziele* verbunden.

Anmerkung 7 zum Begriff: Ein Informationssicherheitsrisiko (*Informationssicherheit* [3.1.1]) kann mit der Möglichkeit verbunden sein, dass *Bedrohungen* (3.4.5) *Schwachstellen* (3.4.6) eines Informationswerts (*Wert* [3.4.2]) oder einer Gruppe solcher *Werte* (3.4.2) ausnutzen und damit interessierten Parteien des Sektors oder Auftraggebern des Sektors Schaden zufügen.

[QUELLE: ISO 31000:2018, 3.1, modifiziert – „Diese Abweichung kann positiv, negativ oder beides sein und kann auf Möglichkeiten und Bedrohungen eingehen, diese verursachen oder durch diese verursacht sein.“ in Anmerkung 1 gelöscht, Anmerkungen 2, 5, 6 und 7 hinzugefügt]

3.4.2

Wert

alles, was für die *Organisation* (3.2.2) von Bedeutung und/oder von Nutzen ist

Anmerkung 1 zum Begriff: Im Zusammenhang mit der *Informationssicherheit* (3.1.1) können zwei Arten von Werten unterschieden werden:

- die Primärwerte:
 - Geschäftsprozesse und -aktivitäten;
 - Informationen;
- die unterstützenden Werte (von denen die Primärwerte abhängen) aller Art, zum Beispiel:
 - Software;
 - Netzwerk;
 - Personal;
 - Standort;
 - Struktur der Organisation.

[QUELLE: ISO/IEC 27002:2022, 3.1.2]

3.4.3

Informationssicherheitsereignis

Vorkommnis, das auf eine mögliche Verletzung der *Informationssicherheit* (3.1.1) oder ein Versagen der *Maßnahmen* (3.4.11) hinweist

[QUELLE: ISO/IEC 27002:2022, 3.1.14]

3.4.4

Informationssicherheitsvorfall

ein oder mehrere zusammenhängende und identifizierte *Informationssicherheitsereignisse* (3.4.3), die den *Werten* (3.4.2) einer *Organisation* (3.2.1) schaden oder ihren Betrieb gefährden können

[QUELLE: EN ISO/IEC 27035-1:2016, 3.4]

3.4.5

Bedrohung

mögliche Ursache eines *Informationssicherheitsvorfalls* (3.4.4), der zu Schaden für ein System oder eine *Organisation* (3.2.1) führen kann

[QUELLE: ISO/IEC 27005, 3.1.9]

3.4.6

Schwachstelle

Schwäche eines *Wertes* (3.4.2) oder einer *Maßnahme* (3.2.1), die durch eine oder mehrere *Bedrohungen* (3.4.5) ausgenutzt werden kann

[QUELLE: ISO/IEC 27000:2018, 3.79]

3.4.7

Risikoszenario

Beschreibung eines möglichen Ereignisses oder Vorfalls, der eine negative Auswirkung auf ein oder mehrere Geschäftsziele (*Ziel* [3.2.2]) haben könnte

Anmerkung 1 zum Begriff: Risikoszenarien haben das Potential, sich auf den Geschäftsprozess und die damit verbundenen Geschäftsanforderungen (*Anforderung* [3.2.5]), die zur Unterstützung der Kerngeschäftsfelder erforderlich sind, auszuwirken.

3.4.8

Angreifer

Akteur, der möglicherweise eine Schwachstelle oder *Bedrohungen* (3.4.5) für seine Zwecke ausnutzt

Anmerkung 1 zum Begriff: Die Begriffe „Angreifer“ und „Bedrohungsagent“ werden synonym verwendet und implizieren Risikofaktoren (*Risiko* [3.4.1]), d. h. vorsätzliche Bedrohungsquellen (*Bedrohung* [3.4.5]).

3.4.9

Angriffspotential

Maß für den Aufwand, der erforderlich ist, um eine *Anfälligkeit* (3.4.6) in einem Ziel auszunutzen

[QUELLE: ISO/IEC 15408-1:2022, 3.8, modifiziert – „Evaluierungsgegenstand“ wurde durch „Ziel“ ersetzt]

Anmerkung 1 zum Begriff: Nach CTI ist das Angriffspotential durch Mittel, Gelegenheiten und Motive des Angreifers gekennzeichnet.

3.4.10

Cybersicherheitsziel

übergeordnete Cybersicherheitsanforderung (*Cybersicherheit* [3.1.2], *Anforderung* [3.2.5])

Anmerkung 1 zum Begriff: ISO/IEC 15408-1 definiert den Begriff in seiner fachlichen Bedeutung als eine „Absichtserklärung, identifizierte *Bedrohungen* (3.4.5) abzuwehren und/oder identifizierte organisatorische Sicherheitsrichtlinien und/oder -annahmen zu erfüllen“.

3.4.11

Maßnahme

Mittel zur Veränderung von *Risiken*

Anmerkung 1 zum Begriff: Maßnahmen umfassen *Prozesse* (3.2.4), *Richtlinien* (3.2.3), Geräte, Methoden oder anderweitige Handlungen, die *Risiken* (3.4.1) verändern.

[QUELLE: EN ISO/IEC 27000:2018, 3.14, modifiziert – Anmerkung 2 zum Begriff wurde gelöscht]

4 Abkürzungen

APL	Angriffspotential (en: attack potential level)
AVA_VAN	Vertrauenswürdigkeitsfamilie nach ISO/IEC 15408-3, die die Anfälligkeitsanalyse adressiert
CAR	Allgemeine Vertrauenswürdigkeitsreferenz (en: Common Assurance Reference)
CC	Allgemeine Kriterien (en: Common Criteria)
CSL	allgemeine Sicherheitsstufe (en: common security level)
CTI	Bedrohungsinformationen (en: Cyberthreat intelligence)
EAL	Vertrauenswürdigkeitsstufe (en: evaluation assurance level)
eUICC	eingebettete UICC (en: embedded Universal Integrated Circuit Card)
IKT	Informations- und Kommunikationstechnologie
IoT	Internet der Dinge (en: Internet of Things)
ISMS	Informationssicherheitsmanagementsystem, nach [3]
MRC	Meta-Risikoklasse (en: meta-risk class)
USIM	universelles Teilnehmeridentitätsmodul (en: Universal Subscriber Identity Module)

5 Sektorales Cybersecurity Assessment

5.1 Anwendung der Methodik für sektorale Cybersecurity Assessments

Die Anwendung der Methodik für sektorale Cybersecurity Assessments beinhaltet die folgenden Aufgaben.

Die erste Phase konzentriert sich darauf, den Sektorkontext als Ausgangspunkt für eine ISO/IEC 27005-konforme Risikobewertung sowie die Folgeschritte der Methodik zu verstehen und zu dokumentieren.

Sie beinhaltet eine Beschreibung der anvisierten sektoralen Dienstleistungen für End- oder Geschäftskunden, der Geschäftsprozesse zur Bereitstellung dieser Dienstleistungen sowie eine Beschreibung der funktionalen Architektur. Auf dieser Basis können Primärwerte, Informationen und funktionale Werte, die für die Geschäftsprozesse entscheidend sind, sowie unterstützende Werte und IKT-Komponenten, die die Informationen und funktionalen Werte unterstützen und schützen, identifiziert werden.

Basierend auf der Dokumentation des Sektorkontexts können Risiken für die Geschäftsziele der Stakeholder-Organisation, beispielsweise aufgrund von Informationssicherheitsvorfällen in Bezug auf die Integrität, Verfügbarkeit oder Vertraulichkeit von Primärwerten, identifiziert und analysiert werden. Für diese Analyse werden

die sektoralen Merkmale der Bedrohungen, insbesondere die Beschreibung des Angriffs und der Angreifer-typen (Cyber Threat Intelligence, CTI, siehe Anhang B), einschließlich einer Bewertung des Angriffspotentials und der Motivation der Angreifer verwendet.

Phase zwei besteht aus aufeinander folgenden Bewertungen.

Zunächst wird im Zuge der Primärwertbewertung und mithilfe einer normalisierten Darstellung (Meta-Risikoklassen, MRC, siehe **Error! Reference source not found.**) eine Einschätzung der im Kontext dokumentierten Risikoinformationen durchgeführt. Diese Beurteilung identifiziert die MRC der Risiken für sektorale Geschäftsprozesse sowie für die Geschäftsziele der Stakeholder-Organisation, die die Primärwerte aufgrund von IKT-Sicherheitsvorfällen beeinträchtigen können.

Auf dieser Grundlage kann die zweite Bewertung der unterstützenden Werte durchgeführt werden, um den Umgang mit den identifizierten und eingestufen Risiken zu unterstützen. Es definiert die Anforderungen an Cybersecurity und Vertrauenswürdigkeit für unterstützende Werte, d. h. IKT-Produkte, -Prozesses oder -Systeme der Stakeholder-Organisation. Dies bezieht sich auf die Identifizierung allgemeiner Sicherheitsstufen (CSL, siehe **Error! Reference source not found.**) und allgemeiner Vertrauenswürdigkeitsreferenzen (CAR, siehe **Error! Reference source not found.**).

Die dritte Phase dient dazu, die im Rahmen des sektoralen Cybersecurity Assessments identifizierten Cybersecurity- und Vertrauenswürdigkeitsanforderungen abzubilden, um Vertrauenswürdigkeitsstufen, Cybersicherheitsziele und Cybersicherheitsstufen des zur Cybersecurity-Zertifizierung geplanten Programms darzustellen.

Error! Reference source not found. gibt einen Überblick über den Ablauf eines sektoralen Cybersecurity Assessments.

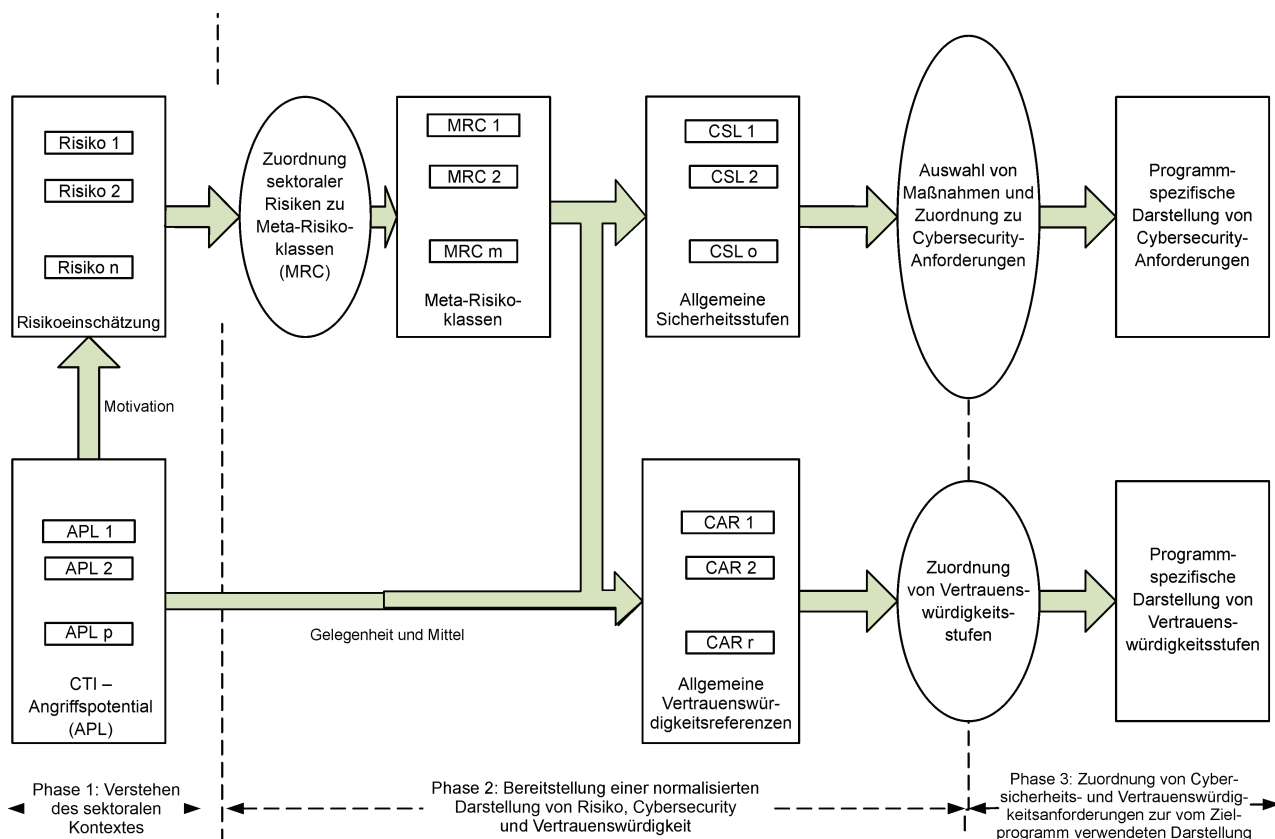


Bild 1 — Sektorales Cybersecurity Assessment

Wie in Bild 1 dargestellt, laufen die Phasen des sektoralen Cybersecurity Assessments nicht nacheinander ab, sondern gehen vielmehr ineinander über. Einige der in diesem Dokument beschriebenen Aktivitäten können zu mehr als einer Phase beitragen. Die Motive, die ein Merkmal des Angriffspotentials darstellen, sollten auch dazu genutzt werden, die Wahrscheinlichkeit eines Vorfalls in Phase 1 zu beurteilen, basierend auf dem Motivationsniveau des Angreifers (siehe 6.3.8), während zwei andere Merkmale, Gelegenheiten und Mittel, auch bei der Bestimmung des CSL (siehe 7.2.3) und des CAR (siehe 7.2.7) in Phase zwei berücksichtigt werden sollten.

5.2 Grundsätze und neue Potentiale

Relevante Informationen, Beziehungen zwischen Parametern

Das sektorale Cybersecurity Assessment erfordert eine gründliche und detaillierte Dokumentation des Sektorkontexts. Auf dieser Grundlage generiert es Informationen zu Risiken in Verbindung mit IKT-Sicherheitsvorfällen, die dann, gemeinsam mit anderen Parametern wie APL, dazu genutzt werden, um angemessene Cybersecurity- und Vertrauenswürdigkeitsanforderungen für die kritischen unterstützenden Werte zu bestimmen.

Ein besonderer Aspekt der Methodik ist, dass die Bewertung in zwei aufeinander folgenden Schritten durchgeführt wird.

Die Bewertungsaktivitäten der Primärwerte folgen dem Risikomanagementstandard ISO/IEC 27005. Dieser bestimmt die Risiken für die Geschäftsziele von Stakeholdern aufgrund von potentiellen Cybersicherheitsvorfällen im Zusammenhang mit Primärinformationen oder funktionalen Werten. Die zweite Bewertung konzentriert sich auf die unterstützenden Werte, d. h. IKT-Systemkomponenten, auf die die Primärwerte angewiesen sind. Diese Bewertung unterstützt die Unterscheidung zwischen unterstützenden Werten, die für die IKT-Sicherheit der Primärwerte entscheidend sind und somit spezielle Cybersecurity- und Vertrauenswürdigkeitsmaßnahmen verdienen, und denjenigen, wo dies nicht erforderlich ist. Kritische unterstützende Werte durchlaufen eine andere Risikobewertungsschleife, die vor der Zuordnung angemessener Cybersecurity- und Vertrauenswürdigkeitsanforderungen zur Risikobehandlung die beabsichtigte Nutzung, die operative Umgebung sowie das relevante Angriffspotential berücksichtigt.

Der Schritt zur Bewertung der unterstützenden Werte kann auch zur Optimierung der Sicherheitsarchitektur des sektoralen IKT-Systems genutzt werden, beispielsweise als Orientierung, wenn es das Ziel ist, sicherheitsrelevante Funktionen in speziellen Komponenten wie Sicherheitselementen oder Hochsicherheitsmodulen zu bündeln.

Bild 2 vermittelt einen Überblick über die vom sektoralen Cybersecurity Assessment benötigten, genutzten und generierten Informationen.

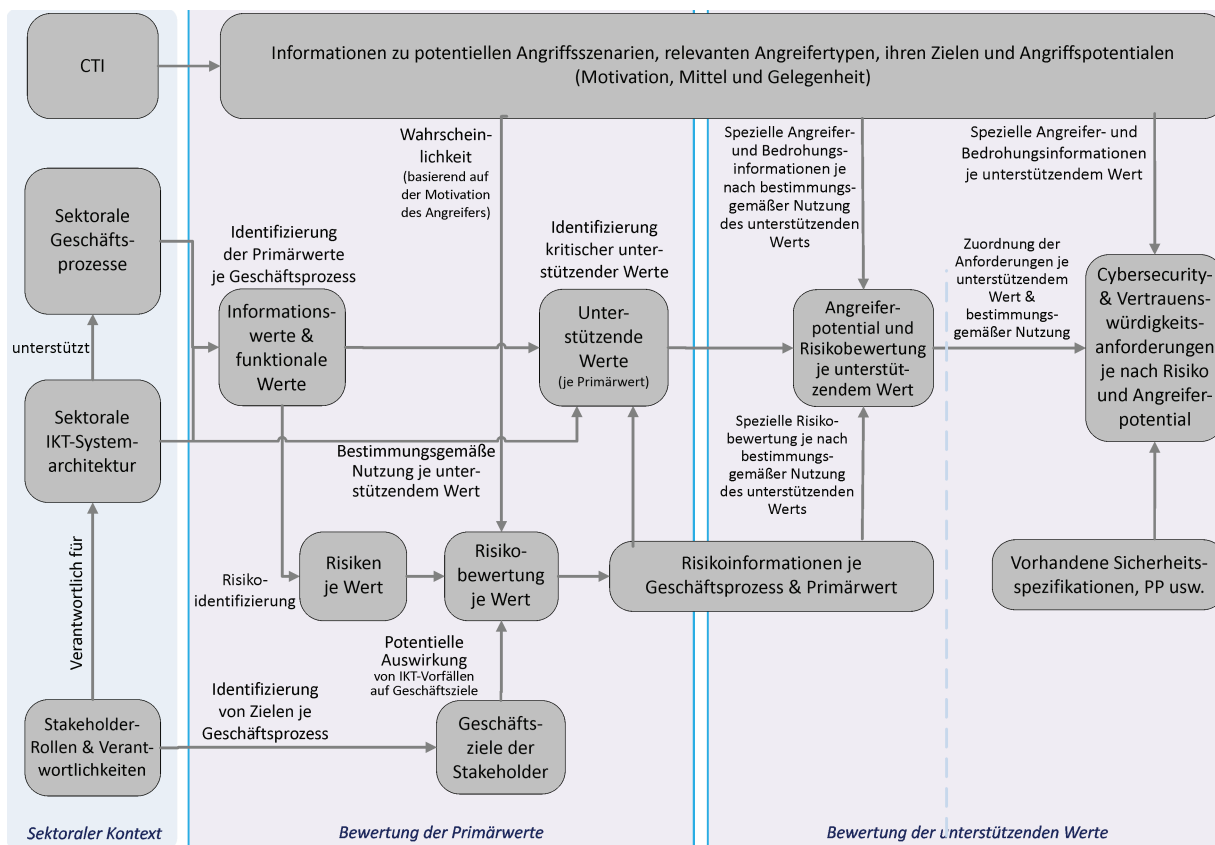


Bild 2 — Überblick über die vom sektoralen Cybersecurity Assessment genutzten und generierten Informationen

Unterstützung einer risikobasierten einheitlichen Implementierung von Cybersecurity und Vertrauenswürdigkeit

Die Definition von Cybersecurity- und Vertrauenswürdigkeitsanforderungen erfolgt auf der Grundlage von Risiken. Zudem kommt Cyber Threat Intelligence (CTI) zur Anwendung, um Informationen zu Angreifertypen und ihrer Motivation, den Mitteln und Gelegenheiten im Hinblick auf Angriffe auf anvisierte IKT-Produkte, -Prozesse und -Dienstleistungen zu erhalten.

Dies führt zu den kritischen Merkmalen des Ansatzes, wie

- „Angriffspotential“ (APL), um Motivation, Mittel und Gelegenheiten der Angreifer zu bewerten,
- „Meta-Risikoklassen“ (MRC), um einen einheitlichen Ansatz zur Risikobewertung zu ermöglichen,
- „allgemeine Sicherheitsstufen“ (CSL), um einen einheitlichen Ansatz bei Cybersicherheitsmaßnahmen zu ermöglichen,
- „allgemeine Vertrauenswürdigkeitsreferenzen“ (CAR), um eine Vergleichbarkeit der Vertrauenswürdigkeitsimplementierungen verschiedener Cybersecurity-Zertifizierungsprogramme zu ermöglichen.

Bei diesem Ansatz entspricht jede allgemeine Sicherheitsstufe (CSL) und jede allgemeine Vertrauenswürdigkeitsreferenz (CAR) einem bestimmten Angriffspotential (APL) und einer bestimmten Meta-Risikoklasse (MRC).

Ermöglichen eines einheitlichen Vertrauenswürdigkeitsansatzes

Das Konzept einer allgemeinen Vertrauenswürdigkeitsreferenz (CAR) leitet sich aus der AVA_VAN-Vertrauenswürdigkeitsfamilie ab, die die Basis für die Anfälligkeitsanalyse in ISO/IEC 15408-3 darstellt. Wie aus AVA_VAN bekannt, ist CAR direkt mit dem Parameter Angriffspotential (APL) verknüpft, der in Übereinstimmung mit dieser Methodik je Angreifertyp basierend auf CTI-Informationen identifiziert wird.

Die Fähigkeit eines Angreifertyps, Angriffe durchzuführen, wird anhand der Angreifertypen des APL bewertet und ist im Wesentlichen unabhängig von der anvisierten unterstützenden Komponente des sektoralen IKT-Systems. Eine einheitliche Implementierung von Vertrauenswürdigkeitsstufen über alle Arten von unterstützten Werten, IKT-Produkte, Prozesse und die jeweiligen Cybersecurity-Zertifizierungsprogramme hinweg kann demzufolge dadurch erreicht werden, dass man die CAR und die APL der Angreifertypen, die motiviert und zum Durchführen von Angriffen in der Lage sein könnten, miteinander verknüpft. Darüber hinaus unterstützt der Ansatz, APL als systemweite Referenz zu nutzen, die Möglichkeit zur Identifizierung der Fähigkeit eines Cybersecurity-Zertifizierungsprogramms, eine spezielle Vertrauenswürdigkeitsstufe zu validieren. Zu diesem Zweck sollte analysiert werden, bis zu welchem APL die Evaluierungsmethodik eines Programms die Widerstandsfähigkeit gegen die Mittel und Gelegenheiten in Verbindung mit einem APL validieren kann.

Die Verwendung von CAR statt von AVA-VAN sollte als wesentlicher Parameter für mehr Flexibilität beim Vergleich verschiedener Implementierungen von Vertrauenswürdigkeitsstufen betrachtet werden. Die CAR ist darauf ausgerichtet, anstelle einer vollständigen Konsistenz die Vergleichbarkeit zwischen Implementierungen zu priorisieren. Dies ermöglicht Abweichungen zwischen den Implementierungen von Vertrauenswürdigkeitsstufen spezifischer Programme. Sie unterstützt die Flexibilität, Marktanforderungen zu folgen, und maximiert die Möglichkeit, Zertifikate verschiedener Cybersecurity-Zertifizierungsprogramme, einschließlich Programme basierend auf Common Criteria und bereits bestehende Branchenprogramme, zu integrieren und gleichzeitig eine angemessene Vergleichbarkeit aufrechtzuerhalten.

ANMERKUNG Obwohl das Konzept von CAR sich auf ISO/IEC 15408 und ISO/IEC 18045 bezieht, steht in diesem Dokument keine Evaluierungsmethodik im Fokus.

Ermöglichen eines Informationsaustauschs zwischen relevanten Standards

Die Definition von Cybersecurity- und Vertrauenswürdigkeitsanforderungen für IKT-Produkte, IKT-Prozesse und IKT-Dienstleistungen spiegelt das mit ihrer bestimmungsgemäßen Nutzung verbundene Cybersicherheitsrisiko wider. Die Bestimmung dieses Risikos wird üblicherweise auf Geschäftssystemebene mithilfe einer auf ISO/IEC 27005 basierenden Informationssicherheitsrisikobeurteilung durchgeführt. Die Spezifizierung der Cybersecurity- und Vertrauenswürdigkeitsanforderungen eines IKT-Produkts wird jedoch üblicherweise mithilfe von ISO/IEC 15408 durchgeführt. Bis jetzt gab es keine Verbindung zwischen den beiden Standards, über die die Informationen auf festgelegte Weise hätten übertragen werden können. Die Spezifizierung von Cybersecurity- und Vertrauenswürdigkeitsanforderungen über Schutzprofile oder Spezifikationen für Sicherheitsfunktionalitäten basierte bisher üblicherweise auf Annahmen des Produktanbieters oder begrenzter Stakeholder-Gruppen und bezog sich somit auf deren Sicht einer „bestimmungsgemäßen Nutzung“, nicht auf Informationen des Eigentümers des Geschäftssystems. Der Ansatz ermöglicht einen Austausch der erforderlichen Informationen zwischen der Geschäftsebene, die ISO/IEC 27005 und verwandte Standards zur Definition risikobasierter Cybersecurity-Anforderungen anwendet, und den Spezifikationen auf Produktebene, deren Definition von Cybersecurity- und Vertrauenswürdigkeitsanforderungen auf ISO/IEC 15408 basiert. Durch die Erweiterung des Ansatzes auf Cybersicherheitsrisiken auf Sektorebene kann ein Austausch spezifischer Informationen und relevanter Anforderungen für sektorale Cybersecurity-Programme hergestellt werden.

Zusammenfassend fungiert dieses Dokument als Bindeglied zwischen bestehenden Risikobewertungsmethoden wie denen, die auf ISO/IEC 27005 basieren, damit ihre Ergebnisse wiederverwendet werden und ein Fokus auf die aktuelle Lücke zwischen Vertrauenswürdigkeitsstufen auf Komponentenebene gerichtet werden kann.

Ermöglichen einer koordinierten Anwendung von Cybersicherheitsmaßnahmen

Der Zweck von Sicherheitsmaßnahmen ist es, Risiken zu mindern und Cybersicherheitsvorfälle zu verhindern. Die Stärke der Maßnahmen, die in Relation zu den allgemeinen Sicherheitsstufen definiert wird, berücksichtigt dabei nicht nur das Risiko, sondern auch das Potential motivierter Angreifer, eine Wirkung zu erzielen.

Basierend auf dem Konzept der allgemeinen Sicherheitsstufen (CSL) ist es zudem möglich, bereits verfügbare Bibliotheken mit implementierten und in Übereinstimmung mit ihrer allgemeinen Sicherheitsstufe möglicherweise skalierten Sicherheitsmaßnahmen (wie in ISO/IEC 27002 beschrieben) zu nutzen. Diese Bibliotheken könnten sowohl Produktanbietern als auch ISMS-Eigentümern dabei helfen, einen bestimmten Cybersicherheitsstandard zu implementieren. Je nach Sektor könnten auch zusätzliche Bibliotheken Berücksichtigung finden, beispielsweise ISO/IEC 27011 für die Telekommunikationsbranche oder ISO/IEC 27019 für Prozesssteuersysteme, wie sie von Energieversorgern genutzt werden.

6 Sektorale Darstellung von Risiken

6.1 Sektorale IKT-Systeme

6.1.1 Sektorale IKT-Systemkomponenten und ihre Beziehungen

Sektorale IKT-Systeme können aus IKT-Produkten und IKT-Prozessen bestehen, die eine IKT-Dienstleistung unterstützen.

Darüber hinaus gibt es IKT-Prozesse, die IKT-Produkte unterstützen, zum Beispiel Produktentwicklungsprozesse. Diese können sich von denjenigen, die IKT-Dienstleistungen unterstützen, unterscheiden.

IKT-Dienstleistungen können sowohl von IKT-Produkten als auch von IKT-Prozessen unterstützt werden, wobei IKT-Produkte auch individuelle IKT-Prozesse unterstützen können.

ANMERKUNG Prozessleistung und Qualitätsmessung liegen außerhalb des Anwendungsbereichs dieses Dokuments.

Die Beziehung zwischen diesen Elementen ist in Bild 3 dargestellt.

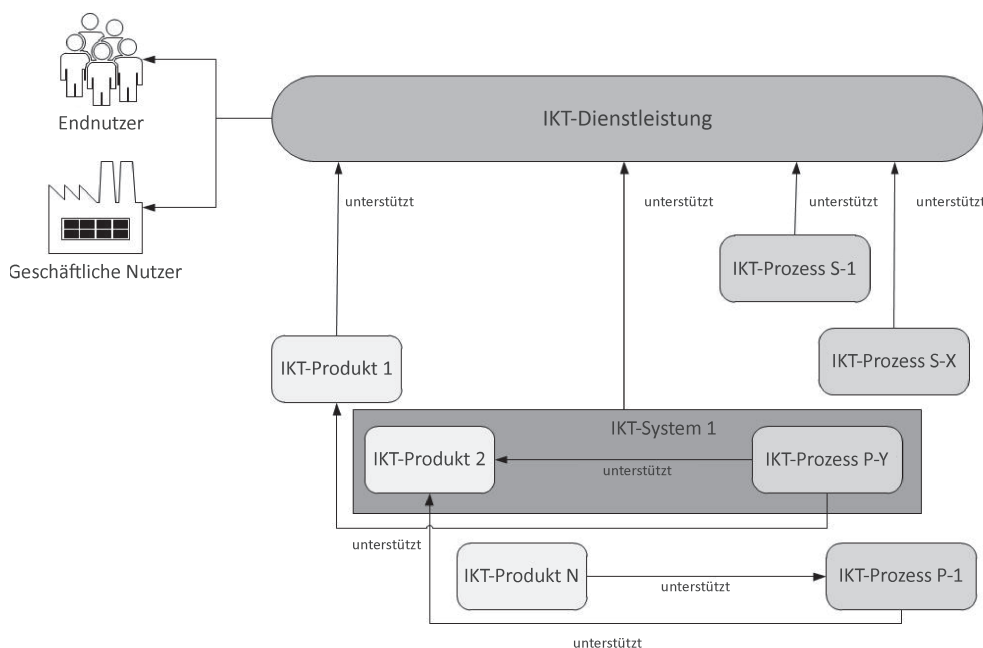


Bild 3 — Beziehung zwischen IKT-Dienstleistungen, IKT-Produkten und IKT-Prozessen

6.1.2 Mehrschichtige Architektur sektoraler IKT-Systeme

Mit Blick auf die Durchführung einer Risikobewertung, Evaluierung und Zertifizierung sollte die IKT-Systemarchitektur definiert werden. Eine Modelldarstellung einer solchen Architektur kann aus mehreren Schichten bestehen. Diese beinhalten:

1) Sektorale IKT-Systeme

Sektorale IKT-Systeme bilden die erste, oberste Schicht der zur Bereitstellung von IKT-Dienstleistungen genutzten Architektur.

Immer wenn für die Cybersicherheit relevante Funktionen eines sektoralen IKT-Systems auf externe IKT-Dienstleistungen angewiesen sind, werden diese als IKT-Infrastrukturdienste betrachtet.

2) IKT-Infrastrukturen

Sektorale IKT-Systeme können auf einer niedrigeren, zweiten Schicht basieren, die von den Infrastrukturdiensten speziell für die Funktionen eines bestimmten Marktsektors kreiert wurde.

IKT-Infrastrukturen können für verschiedene Märkte, Anwendungen und Endnutzerleistungen genutzt werden. Obgleich nicht sektorspezifisch, können sie in sektorale IKT-Systeme integriert werden.

BEISPIEL Zu IKT-Infrastrukturen gehören Mobilfunknetzte, Cloud-Dienste sowie Zahlungs- oder Identitätsmanagementdienste.

Man könnte auch sagen, dass IKT-Infrastrukturen für von ihnen unterstützte sektorale IKT-Systeme IKT-Dienstleistungen bereitstellen. Aus geschäftlicher Sicht kann dies auch als eine Beziehung zwischen anderweitig nicht verbundenen Organisation betrachtet werden, wobei eine Seite die Rolle des IKT-Infrastrukturdienstleisters übernimmt und die andere Seite die des geschäftlichen Nutzers.

Externe IKT-Infrastrukturdienste sollten ebenfalls bei der Risikobewertung berücksichtigt werden, da sie für die Cybersicherheits- und Vertrauenswürdigkeitsstufen des sektoralen IKT-Systems ausschlaggebend sein können.

3) Generische IKT-Produkte

IKT-Produkte können sowohl in sektoralen IKT-Systemen als auch in IKT-Infrastrukturen zur Anwendung kommen. Aus architektonischer Sicht kreieren sie eine weitere, separate Schicht in der Modelldarstellung.

IKT-Produkte können sowohl in sektoralen IKT-Systemen als auch in IKT-Infrastrukturen zur Anwendung kommen. Diese IKT-Produkte sollten als separate Schicht in der Modelldarstellung berücksichtigt werden.

Generische IKT-Produkte, die in größerer Anzahl auftreten, werden deshalb einer Zertifizierung unterzogen.

Die Beziehungen zwischen den Schichten eines sektoralen IKT-Systems sind in Bild 4 dargestellt.

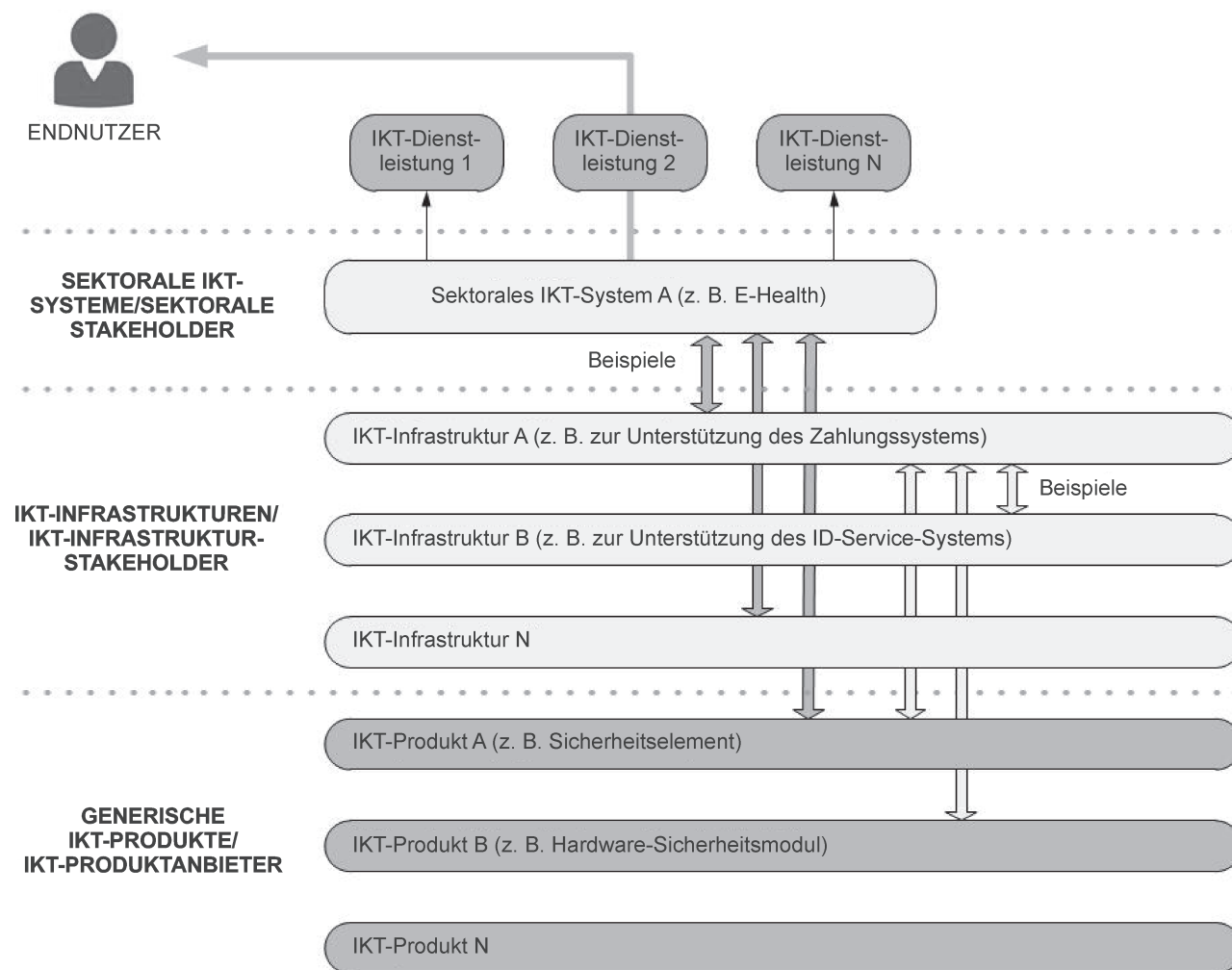


Bild 4 — Schichten eines sektoralen IKT-Systems

IKT-Infrastrukturen und sektoralen IKT-Systeme können miteinander kombiniert werden.

BEISPIEL 5G-Netzwerk-, Zahlungs- und Identitätsmanagementdienste werden üblicherweise mit sektoralen IKT-Systemen integriert und bieten Nutzern IKT-Dienstleistungen.

Aus Sicht der Cybersicherheitsevaluierung und -zertifizierung ist es wichtig, nicht nur die technische Interaktion zwischen diesen Bausteinen des gesamten sektoralen IKT-Systems zu berücksichtigen, sondern auch die Zuweisung der Verantwortlichkeiten innerhalb; da die Eigentümer jedes Bausteins üblicherweise Risikobewertungen durchführen, geeignete Sicherheitsmaßnahmen implementieren und eine Evaluierung und Zertifizierung auf ihrer Ebene unterstützen.

Dabei sollte ein zentraler Unterschied zwischen IKT-Infrastrukturen und IKT-Produkten beachtet werden. Die Eigentümer von IKT-Infrastrukturen sind für die Definition, die Implementierung und den Betrieb der Infrastruktur verantwortlich. Auf der anderen Seite sind diejenigen, die IKT-Produkte kaufen, für die Integration und den Betrieb des Produkts in Übereinstimmung mit seiner bestimmungsgemäßen Nutzung verantwortlich; das bedeutet, dass Anbieter in dem Fall dafür verantwortlich sind, den Stakeholdern von sektoralen IKT-Systemen oder IKT-Infrastrukturen evaluierte und zertifizierte IKT-Produkte bereitzustellen.

6.1.3 Risikobasierte Definitionen von Cybersecurity- und Vertrauenswürdigkeitsanforderungen in sektoralen Systemen

Sektorale Risikobewertungen sind der Schlüssel für die Formulierung von Cybersecurity- und Vertrauenswürdigkeitsanforderungen zur Unterstützung von in verschiedenen Sektoren genutzten IKT-Infrastrukturen und IKT-Produkten, und für diejenigen IKT-Produkte und IKT-Prozesse, die, von sektoralen IKT-Systemen intern genutzt werden.

Die übergeordnete Beschreibung der Beziehungen zwischen verschiedenen Stakeholdern lauten wie folgt:

- 1) Die sektoralen Stakeholder sollten die Cybersecurity- und Vertrauenswürdigkeitsanforderungen auf Grundlage einer Risikobewertung aus Sicht der Geschäftsziele des jeweiligen Sektors identifizieren und gleichzeitig rechtliche oder behördliche Anforderungen berücksichtigen.
- 2) Die sektoralen Stakeholder sollten ihre Anbieter von IKT-Infrastrukturdiensten, IKT-Prozessen und IKT-Produkten über die bestimmungsgemäße Nutzung sowie dazugehörige Anforderungen an diese Infrastrukturdienste, IKT-Prozesse oder IKT-Produkte informieren.
- 3) Auf Grundlage dieser sektoralen Informationen können Anbieter die Cybersecurity- und Vertrauenswürdigkeitsanforderungen all ihrer anvisierten Sektoren berücksichtigen und Infrastrukturdienste, IKT-Produkte und IKT-Prozesse definieren, die an diese Sektoren vermarktet werden können.
- 4) Anbieter sollten die Konformität ihrer IKT-Infrastrukturdienste, -Produkte und -Prozesse mit den sektoralen Anforderungen durch geeignete Maßnahmen wie Service Level Agreements, Spezifikationen und, falls eine Cybersecurity-Zertifizierung gefordert wird, Zertifikaten bestätigen.
- 5) Sollten Anbieter von IKT-Infrastrukturdiensten, IKT-Produkten oder IKT-Dienstleistungen nicht alle sektoralen Anforderungen erfüllen können, sollte das sektorale Cybersecurity Assessment die daraus resultierenden Risiken identifizieren und geeignete Maßnahmen festlegen.

6.1.4 Relevanz der sektoralen IKT-Systemarchitektur für die Risikobewertung

Die Bewertung der Cybersicherheitsrisiken basiert auf den relevanten Geschäftsprozessen und den entsprechenden Zielen der sektoralen Stakeholder, die durch cybersicherheitsrelevante Ereignisse oder Vorfälle beeinträchtigt werden könnten. Diese Überlegungen konzentrieren sich auf geschäftliche, staatliche oder gesellschaftliche Sichtweisen des sektoralen IKT-Systems und sollten das sektorale Rollenmodell und die Arbeitsteilung zwischen den Stakeholdern wie unter 6.1.3 beschrieben widerspiegeln.

Für die Definition der Anforderungen zum geplanten Cybersecurity-Zertifizierungsprogramm im Sinne von Cybersicherheits- und Vertrauenswürdigkeitsstufen sollte jedoch ein technischer Blickwinkel aus Sicht der IKT-Systemarchitektur eingenommen werden. Diese Anforderungen zielen auf sektorale IKT-Subsysteme, IKT-Produkte, IKT-Prozesse und IKT-Dienstleistungen ab, die die Implementierung relevanter Geschäftsprozesse auf sektoraler IKT-Systemebene unterstützen.

Um zwei Notwendigkeiten auf einheitliche Weise zu implementieren, sollte eine angemessene Relevanz zwischen sektoralen IKT-Systemen und wertbasierter Risikobewertung in Betracht gezogen werden.

In sektoralen IKT-Systemen stellen Primärwerte im Prinzip Informationen dar, während unterstützende Werte kritische Systemelemente darstellen, die es den Primärwerten ermöglichen, die Geschäftsprozesse effizient und wirksam zu unterstützen.

Es ist wichtig, anzumerken, dass nicht notwendigerweise eine direkte Beziehung zwischen unterstützenden Werten und Primärwerten besteht; ein unterstützender Wert kann für mehr als einen Primärwert von Bedeutung sein, und ein Primärwert kann von mehreren unterstützenden Werten gestützt werden.

Die Beziehung zwischen Geschäftsprozessen, sektoraler IKT-Systemarchitektur, Primärwerten und unterstützenden Werten ist in Bild 5 dargestellt.

Geschäftliche Ebene

Gruppe von Geschäftsprozessen, die ein oder mehrere sektorale Geschäftsziele unterstützen

Sektorale IKT-Systemebene

Primärwerte

Informationswerte, die einen oder mehrere sektorale Geschäftsprozesse unterstützen, um ein oder mehrere Geschäftsziele zu erreichen

Unterstützende Werte

IKT-Produkte, IKT-Prozesse, die einen oder mehrere Primärwerte unterstützen

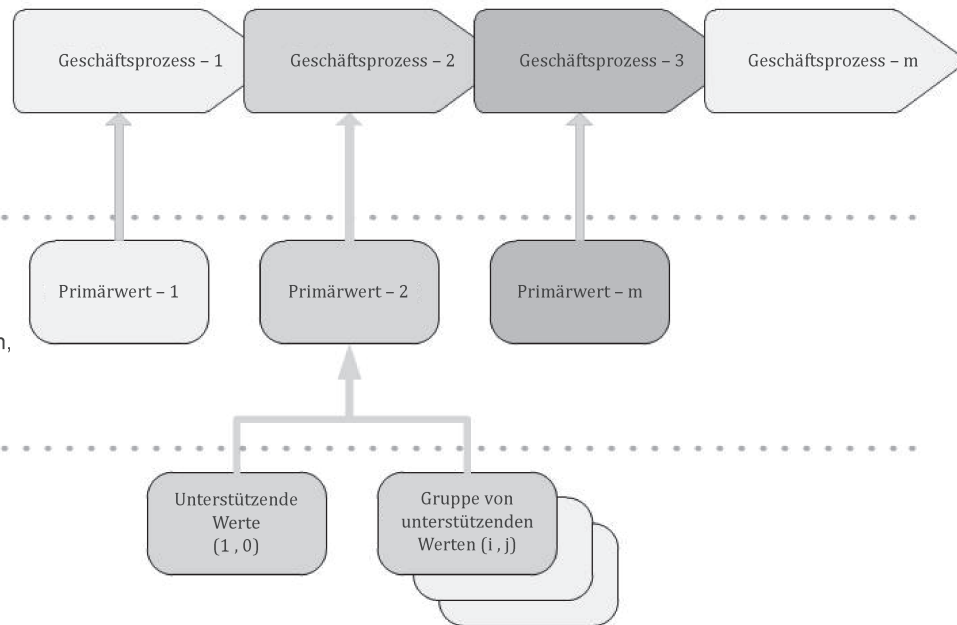


Bild 5 — Beziehung zwischen Geschäftsprozessen, Primärwerten und unterstützenden Werten

BEISPIEL Stellen wir uns einen Geschäftsprozess vor, der über ein 5G-Netzwerk Datendienste für Kunden bereitstellt. Aus Sicht des sektoralen IKT-Systems (5G-Netzwerk) sind die kryptographischen Schlüssel der Mobilfunkteilnehmer Primärwerte. Die unterstützenden Werte der kryptographischen Schlüssel sind:

- SIM zur Speicherung der kryptographischen Schlüssel der Teilnehmer;
- UDM/ARPF – die „Authentication Credential Repository and Processing Function“ (ARPF) ist ein Element des einheitlichen Datenmanagements (UDM, en: unified data management), der Netzwerkfunktion zur Speicherung und Verwaltung von Teilnehmer- und Authentifizierungsdaten.

6.1.5 Cybersecurity-Zertifizierung sektoraler IKT-Systeme

Das sektorale IKT-System kann sehr komplex sein. Darüber hinaus kann die Implementierung der erforderlichen Funktionen sich von Stakeholder-Organisation zu Stakeholder-Organisation erheblich unterscheiden. Eine derartige Komplexität und Diversität verhindert in der Regel die Definition einer eindeutigen technischen Spezifikation wie sie für IKT-Produkte genutzt wird und üblicherweise für IKT-Produktzertifizierungen erforderlich ist.

Stakeholder sektoraler IKT-Systeme sollten die Anwendbarkeit verschiedener Cybersecurity-Zertifizierungsmaßnahmen in Betracht ziehen, um ihre Konformität mit sektoralen Cybersecurity- und Vertrauenswürdigkeitsanforderungen zu demonstrieren.

Der ISMS-basierte Ansatz bei Cybersecurity und Zertifizierung kann in sektoralen Organisationen Anwendung finden, da das ISMS Geschäftsprozesse, die durch sektorale IKT-Systeme gestützt werden, welche die Mehrzahl der IKT-Produkte und IKT-Prozesse nutzen, abdeckt.

Der Umfang eines sektoralen ISMS kann nach den Anforderungen der Organisation gewählt werden und kann sich auf die Geschäftsprozesse eines bestimmten IKT-Systems beschränken.

BEISPIEL Der Geschäftsprozess für das Teilnehmermanagement, der von einem bestimmten IKT-System unterstützt wird, kann als Subjekt eines sektoralen ISMS betrachtet werden.

Die IKT-Produktzertifizierung kann IKT-Produkte betreffen, die wichtige Funktionen des sektoralen IKT-Systems unterstützen, und einen festgelegten Cybersecurity- und Vertrauenswürdigkeitsstandard erfordern.

Die Zertifizierung sowohl der sektoralen Schicht als auch der IKT-Systeme der Stakeholder-Organisation basiert für gewöhnlich auf ISMS-Standards wie EN ISO/IEC 27001. Diese bieten einen bewährten und praktischen Ansatz für das Cybersecurity- oder Informationssicherheitsmanagement und sind in vielen Sektoren gut etabliert. Sie unterstützen jedoch nicht das Konzept festgelegter Vertrauenswürdigkeitsstufen, wie sie von Standards für IKT-Sicherheitsevaluierungen speziell für IKT-Produkte bereitgestellt werden, wie EN ISO/IEC 15408. Diese Anforderungen sollten an das ISMS des Stakeholders als „externe Anforderungen“ kommuniziert und berücksichtigt werden, wenn eine geeignete Informationssicherheitsstufe im ISMS festgelegt wird. In diesen Fällen sollte eine einheitliche Implementierung von Cybersecurity- und Vertrauenswürdigkeitsanforderungen über alle IKT-Systeme der sektoralen Stakeholder-Organisationen hinweg unterstützt werden, indem die Sicherheitsarchitektur und das Zertifizierungskonzept der sektoralen Systeme definiert wird.

Es sollte angemerkt werden, dass nicht alle Stakeholder in der Lage sind, geeignete Cybersecurity- und Vertrauenswürdigkeitsanforderungen in sektoralen multiorganisatorischen Umgebungen zu identifizieren.

BEISPIEL 1 Die Hersteller von Komponenten von IKT-Produkten wissen für gewöhnlich nicht, wo ihre Komponenten zum Einsatz kommen.

BEISPIEL 2 Im Industriebereich führt der Integrator eine Risikobeurteilung durch und entscheidet dann, ob die Sicherheitsfunktionalität der Komponente ausreichend ist oder vor ihrem Einsatz zusätzliche Maßnahmen erforderlich sind.

In allen Fällen sollten die Definitionen der Cybersecurity- und Vertrauenswürdigkeitsanforderungen für sektorale IKT-Systeme und für Systeme, die externe IKT-Infrastrukturdienste unterstützen, sowie für generische IKT-Produkte vergleichbar sein, um eine einheitliche Implementierung der Vertrauenswürdigkeitsstufen sicherzustellen.

6.2 Einheitliche sektorale Risikobewertung

Ein in Verbindung mit einem Sektor und seinen IKT-Produkten, IKT-Prozessen und IKT-Dienstleistungen stehendes Risiko sollte im Kontext jedes Angreifers bewertet werden, der die Cybersicherheit zu verletzen versucht. Das bedeutet, dass das Risiko direkt von der potentiellen Wirkung abhängt, die ein Angreifer auf ein laufendes sektorales IKT-System hat.

Angreifer können anhand ihrer Fähigkeiten charakterisiert werden, d. h. ihrer Motivation, Mittel und Gelegenheiten. Das Spektrum potentieller Angreifer sowie ihrer Fähigkeiten hat einen großen Einfluss auf die Risiken, denen jedes IKT-System ausgesetzt ist.

BEISPIEL Hochqualifizierte Angreifer, die einen kritischen Infrastruktursektor wie beispielsweise den Energiesektor im Visier haben, können nicht nur über die Ressourcen zur Durchführung eines derartigen Angriffs verfügen, wenn es sich z. B. um einen staatlich geförderten Akteur handelt, sondern zudem auch die Gelegenheiten zur Durchführung des Angriffs mit großem Erfolg identifizieren.

Um eine gewisse Einheitlichkeit bei der Zertifizierung sowie eine sektorübergreifende Vergleichbarkeit aufrechtzuerhalten, ist es unerlässlich, vergleichbare Risikoniveaus als Grundlage für die Evaluierung zu nutzen. Aktuell standardisieren jedoch nicht einmal Organisationen innerhalb desselben Sektors ihre Methoden zur Risikoanalyse und Risikobewertung. Überdies können unterschiedliche sektorale Einschätzungen hinsichtlich Risikotoleranz und Risikobereitschaft während der Risikobewertung berücksichtigt werden. Wird eine derartige Flexibilität ermöglicht, könnten Sektoren vergleichbare Risiken unterschiedlich bewerten, was zu verschiedenen sektoralen Cybersecurity- und Vertrauenswürdigkeitsanforderungen führt, ohne dass das Ziel der Einheitlichkeit davon berührt wird.

BEISPIEL Als Risikoeigentümer von Mobilfunknetzen sind Mobilfunknetzbetreiber dafür verantwortlich, den Teilnehmerzugang zu ihren mobilen Diensten zu sichern. Werden SIM-Karten für das Hosting der Teilnehmerzugangsdaten genutzt, enthalten die Mobilfunkdienste den Kauf und die Personalisierung der SIM-Karten. Auf diese Weise können die Betreiber die Sicherheitsimplementierung der SIM-Karte und die damit verbundenen Risiken vollumfänglich kontrollieren. Mit der Einführung der eSIM, die für mehrere Identitäten und verschiedene Dienste ausgerüstet ist, wurde

auch ein neuer Prozess zur Personalisierung mit Teilnehmerdaten eingeführt. Dabei sind neue Stakeholder involviert, an die diese Verantwortlichkeiten übertragen werden. Bei einem eSIM-basierten Szenario hat der Mobilfunknetzbetreiber keine direkte vertragliche Beziehung mit dem eSIM-Anbieter und somit keine direkte Kontrolle darüber, wie die Sicherheitsanforderungen der eSIM konzipiert und implementiert werden. In einem derartigen Szenario hängt das Risiko des Mobilfunknetzbetreibers von der sicheren Implementierung kritischer Funktionen und Aufgaben durch andere Stakeholder ab. Eine risikobasierte Identifizierung der Cybersecurity- und Vertrauenswürdigkeitsanforderungen ist deshalb für alle beteiligten Stakeholder-Organisationen unerlässlich, um eine einheitliche Adressierung der Anforderungen und Implementierung geeigneter Maßnahmen zu erreichen.

Eine Reihe übergeordneter Risikoklassen bereitzustellen ist notwendig, um die individuell von den Sektoren genutzten Risikoniveaus oder von den Organisationen übernommenen Risikobewertungsmethoden abzubilden. Trotz der unterschiedlichen Risikoeinschätzung verschiedener Stakeholder können all diese Risiken in den sogenannten „Meta-Risikoklassen“ (MRC) abgebildet werden. Diese MRCs bieten eine normalisierte Risikodefinition, die in allen sektoralen Programmen zur Anwendung kommen sollte. Sie werden unter 7.1 diskutiert.

Diese Risikoklassen sollten die Grundlage für eine einheitliche Definition von Cybersecurity- und Vertrauenswürdigkeitsanforderungen bilden, über verschiedene Cybersecurity-Zertifizierungsprogramme hinweg.

6.3 Durchführung einer sektoralen Risikobewertung

6.3.1 Allgemeines

Sektorale Risikobewertungen sollten von der koordinierenden Einheit des Sektors oder dem Entwickler eines sektoralen Cybersecurity-Zertifizierungsprogramms auf einer übergeordneten Ebene durchgeführt werden. Beide müssen relevante Stakeholder direkt aus dem Sektor und den dazugehörigen Organisationen involvieren.

Sektorale Risikobewertungen haben zwei Ziele:

- 1) Identifizierung risikobasierter Anforderungen für unterstützende Werte, basierend auf ihrer bestimmungsgemäßen Nutzung;
- 2) Marktakzeptanz durch die Herstellung eines Zusammenhangs zwischen Cybersecurity- und Vertrauenswürdigkeitsanforderungen (und ihren Kosten für die Stakeholder) und den Geschäftsrisiken der Stakeholder, die durch eine Implementierung dieser Anforderungen gemindert werden können.

Sektorale Risikobewertungen konzentrieren sich auf die für die Geschäftsziele entstehenden Risiken, die die sektoralen Stakeholder den von ihnen mithilfe des sektoralen IKT-Systems bereitgestellten sektoralen Dienstleistungen zuordnen. Die dem Sektor von der IKT-Infrastruktur zur Verfügung gestellten IKT-Produkte, IKT-Prozesse und IKT-Dienstleistungen werden aus Sicht der sektoralen Risikobewertung als unterstützende Werte angesehen und könnten entweder von einer einzelnen Stakeholder-Organisation innerhalb eines Sektors oder auf Sektorebene von der koordinierenden Einheit eingesetzt werden. Die im Rahmen der sektoralen Risikobewertung zu berücksichtigenden Risikoquellen und Risikoeigentümer beinhalten:

- die der Stakeholder und der koordinierenden Einheit, die das IKT-Produkt, die IKT-Dienstleistung oder den IKT-Prozess nutzen („geschäftliche Nutzer“);
- die des Sektors und seiner Stakeholder – einschließlich der Organisationen, die Teil der sektoralen Lieferkette sind;
- die der Gesellschaft insgesamt, sowohl auf europäischer als auch auf internationaler Ebene.

Das Gesamtkonzept der Risikobewertung in sektoralen Systemen ist in Bild 6 dargestellt. Spezifische Elemente der sektoralen Risikobewertung werden in den folgenden Abschnitten diskutiert.

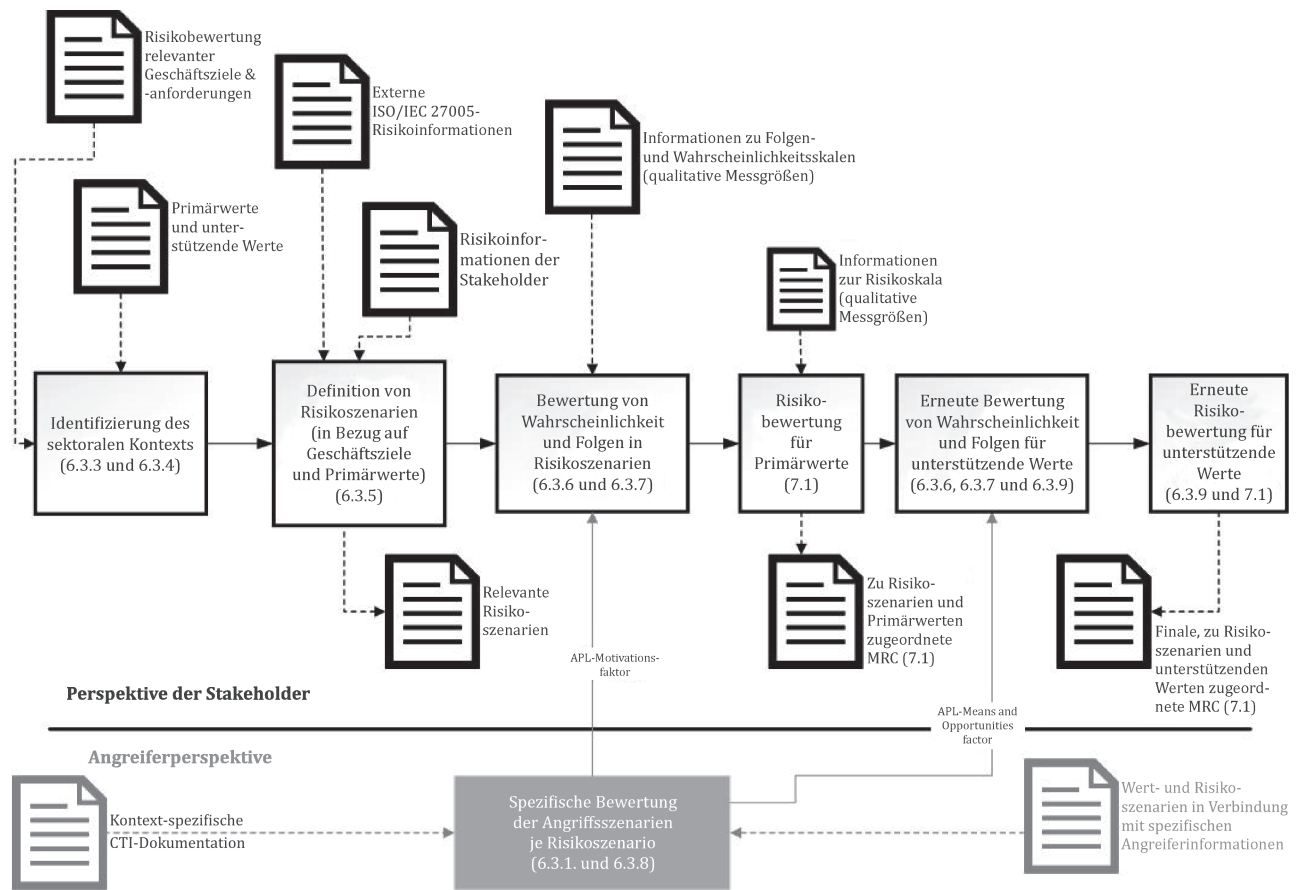


Bild 6 — Sektorale Risikobewertung

6.3.2 Wahl des Ansatzes

Im Rahmen einer übergeordneten Risikobewertung wird empfohlen, bei der Schätzung der Risikoniveaus, die in Abhängigkeit von den Folgen und Wahrscheinlichkeiten betrachtet werden, eine qualitative Methode zu nutzen und eine festgelegte Skala von qualifizierenden Attributen anzulegen (z. B. hoch, mittel, niedrig).

Eine detailliertere Beschreibung von Methoden zur Risikoidentifizierung und zur systematischen Analyse von Risikoquellen mittels quantitativer, qualitativer oder gemischter Methoden ist in ISO/IEC 27005 verfügbar.

Ein Beispiel dieses Ansatzes ist in Anhang A dargestellt.

6.3.3 Identifizierung von Geschäftsprozessen, -zielen und -anforderungen

Der erste Schritt besteht darin, die Geschäftsprozesse zu identifizieren. Im Anschluss sollten relevante Geschäftsziele und Geschäftsanforderungen identifiziert werden. Die sektoralen IKT-Systeme und ihre Architekturen sind so definiert, dass sie die Geschäftsprozesse und die damit verbundenen Geschäftsziele unterstützen. Primärwerte und unterstützende Werte sollten den relevanten Geschäftsprozessen auf Grundlage der verschiedenen Schichten, die eine Architektur unterstützender Systeme beschreiben, zugeordnet werden. Cybersicherheitsrisiken sollten sich auf die Werte beziehen, und damit indirekt auf die Geschäftsprozesse.

6.3.4 Identifizierung von Primärwerten und unterstützenden Werten

Zunächst einmal können Geschäftsprozesse und die damit verbundenen Ziele durch Informationssicherheitsrisiken im Zusammenhang mit den Primärwerten beeinträchtigt werden. Mögliche Folgen sollten aufgrund der

von sektoralen Stakeholdern zur Verfügung gestellten Risikoinformationen gesammelt werden oder über ein ISO/IEC 27005-konformes Risikomanagementtool generiert werden.

Die konsolidierten Einschätzungen der Stakeholder zu den Folgen und Wahrscheinlichkeiten, dass sich ein Risiko materialisiert, sollten mit der Sicht der Angreifer kombiniert werden, da ihre Motivation und ihre Fähigkeit, Angriffe durchzuführen, die die Primärwerte kompromittieren können, die Wahrscheinlichkeit festlegen.

Im nächsten Schritt sollten die unterstützenden Werte, auf die die Primärwerte angewiesen sind, berücksichtigt werden, um die Cybersecurity- und Vertrauenswürdigkeitsanforderungen für IKT-Systeme, IKT-Produkte, IKT-Dienstleistungen und IKT-Prozesse zu definieren. Die Risikoinformation, die auf einen unterstützenden Wert zutrifft, hängt von der Bewertung der Primärinformation oder des funktionalen Werts ab, der vom unterstützenden und zu bewertenden Wert unterstützt wird. Für eine genauere Risikobewertung der zur Durchführung von Angriffen vorhandenen Fähigkeiten und Ressourcen der relevanten Angriffertypen werden das Angriffspotential (APL), die bestimmungsgemäße Nutzung sowie die Betriebsumgebung berücksichtigt. Die Definition des APL und die Methode zur Bestimmung des APL sind in B.5 beschrieben.

6.3.5 Definition von Risikoszenarien

Risiko wird in Abhängigkeit von den bewerteten Folgen und der Wahrscheinlichkeit, dass sich das Risiko materialisiert, betrachtet.

Das Risikoszenario ist eine Methode, die genutzt wird, um die Risikobewertung zu vereinfachen, indem die Anzahl der möglichen Risikovarianten begrenzt und die Geschäftsziele und -anforderungen mit den Risiken abgeglichen werden.

Die Beschreibung eines Risikoszenarios beinhaltet die Dokumentation der relevanten Parameter aus den folgenden Bereichen:

- Geschäftsperspektive: Anvisierter Geschäftsprozess, involvierte Stakeholder und ihre Ziele und Anforderungen für den anvisierten Geschäftsprozess.
- Architekturperspektive: Primärwert (Information und Funktion) im Zusammenhang mit dem anvisierten Geschäftsprozess, unterstützende Werte des Primärwerts.
- Angreiferperspektive: Angriffertypen (siehe B.2 für weitere Einzelheiten), die in der Lage und motiviert sein können, Angriffe auf den Primärwert durchzuführen. Alle relevanten Informationen sind in Risikoszenarien zusammengefasst, die dem Primärwert zugeordnet werden sollten.

Die Identifizierung von Risikoszenarien sollte in Verbindung mit einem Geschäftsprozess und einem für die Ziele des Geschäftsprozesses relevanten Primärwert durchgeführt werden. Im Anschluss wird ein Angriffsszenario, das möglicherweise über einen Angriff auf den Primärwert zu einem Vorfall führen könnte, hinzugefügt (siehe 6.3.8).

Es sollte angemerkt werden, dass Angriffe auf die Cybersicherheit für gewöhnlich Werten und nicht Geschäftsfunktionen gelten; es ist in der Regel nicht möglich, relevante Risikoszenarien auf Geschäftsziel-, Prozess- oder Anforderungsebene zu identifizieren. Die Auswirkungen der Risikoszenarien auf die Geschäftsziele können deshalb nur durch eine genaue Bewertung auf der Ebene der Primärwerte oder der unterstützenden Werte erkannt werden.

6.3.6 Bewertung der Folgen in Risikoszenarien

Nach der Identifizierung der Risikoszenarien sollte es für die Stakeholder möglich sein, die potentiell im Falle eines Risikoszenarios eintretenden Folgen für die Geschäftsziele einzuschätzen.

Es lohnt sich, anzumerken, dass ein Risikoszenario mehrere Geschäftsziele eines Stakeholders betreffen kann und dass verschiedene Stakeholder eines Sektors eine unterschiedliche Sicht der damit verbundenen Folgen haben können.

Die Stakeholder sollten mehrere, von den Auswirkungen betroffene Bereiche in Betracht ziehen, einschließlich:

- Geschäftsprozesse und -funktionalitäten;
- Benutzer;
- die Art der verarbeiteten Daten;
- Reputation und Vertrauen;
- Einhaltung gesetzlicher, behördlicher und vertraglicher Anforderungen;
- Gesundheit und Leben.

Da Stakeholder je nach ihren Geschäftszielen eine unterschiedliche Sicht der potentiell durch ein Risikoszenario verursachten Auswirkungen haben und unterschiedliche Arten und Bewertungen der Folgen gewählt haben könnten, sollte eine Moderation durchgeführt werden, mit dem Ziel, zu einer gemeinsamen Sichtweise zu gelangen.

Die erste Bewertung sollte anhand von Überlegungen zu relevanten Angreifern und ihrem Potential weiter verfeinert werden, da dies die Bewertung der Folgen, wie unter 6.3.8. beschrieben, beeinflussen kann.

Sowohl die erste als auch die finale Bewertung der Folgen sollte dokumentiert werden.

Um ihre sektorübergreifende Vergleichbarkeit sicherzustellen, sollte eine generische, qualitative Folgenskala erstellt werden, die zumindest vereinbarte Werte für die kritischen Risikokategorien (z. B. für Gesundheit und Leben) enthält, die nicht unterschritten werden sollten.

Beispiele für eine qualitative Skala und ihre Folgenstufen sind in A.1 dargestellt.

6.3.7 Bewertung der Wahrscheinlichkeit in Risikoszenarien

Informationen zur Wahrscheinlichkeit können aus unterschiedlichen Quellen bezogen werden:

- Die Erfahrung der Stakeholder und/oder der Organisation, die alle am sektoralen IKT-System beteiligten Parteien koordiniert.
- Die Analyse der potentiellen Angreifer, ihrer Motivation, Mittel und Gelegenheiten. Derartige Informationen sollten wie unter beschrieben von der CTI bereitgestellt werden und werden durch das Risikoszenario referenziert, möglicherweise durch die Entwicklung relevanter Angriffsszenarien und die Zuordnung relevanter Angriffspotentiale zu diesen Szenarien.
- Ist ein Risikoszenario nicht sektorspezifisch, kann die Wahrscheinlichkeit auf der Grundlage von Informationen zu ähnlichen Angriffen in anderen IKT-Systemen mit ähnlichen Lieferketten geschätzt werden.

ANMERKUNG Es gibt zusätzliche Informationsquellen wie Computer Security Incident Response Teams (CSIRT), Information Sharing and Analysis Centers (ISAC), offene Repositorys und kommerzielle Listen.

Die vorgenannten Informationen werden auf andere Weise gemessen oder bewertet; im Allgemeinen kann die Erfahrung von Stakeholdern mit früheren Vorfällen zu einer messbaren Wahrscheinlichkeit führen (zum Beispiel die Häufigkeit einer bestimmten Angriffsform während eines Jahres), besonders im Fall von sektoralen IKT-Systemen, die bereits eine Zeit lang laufen.

BEISPIEL Weiß der Sektor, dass dazugehörige Organisationen gemeinsam durchschnittlich mehr als einen Distributed-Denial-of-Service-/DDOS-Angriff je Jahr melden, dann würde die Wahrscheinlichkeit, dass ein derartiger Vorfall den Geschäftsbetrieb und die Funktionalitäten beeinträchtigt, als „hoch“ oder ähnlich eingestuft werden. Sind andererseits bisher noch keine DDOS-Angriffe innerhalb des Sektors verzeichnet worden, würde die Wahrscheinlichkeit üblicherweise als „niedrig“ oder ähnlich eingestuft werden wollen.

Abgesehen von den eigenen Erfahrungen sollte der Sektor auch die Erfahrungen anderer Sektoren – innerhalb der eigenen Lieferkette – berücksichtigen. Wie anhand des Beispiels mit den DDOS-Angriffen gezeigt, ist es deshalb, auch wenn der Sektor selbst nie einen Vorfall erlebt hat, wahrscheinlich, dass andere innerhalb der Lieferkette damit Erfahrungen gemacht haben – und die Wahrscheinlichkeit sollte somit höher als vorher eingestuft werden.

Darüber hinaus sollten auch weitreichendere Erfahrungen und ihre Anwendbarkeit auf den Sektor berücksichtigt werden. Der derzeitige Stand der Technik zeigt, dass mehr und mehr Cyberangriffe wiederverwendet werden, d. h. sie zielten ursprünglich lediglich auf bestimmte Sektoren ab und wurden dann weiterverkauft und für andere Ziele eingesetzt.

Andere Informationen sind von besserer Qualität, wie zum Beispiel Informationen zur Motivation und zu den Fähigkeiten eines Angreifers, ein sektorales IKT-System anzugreifen. Die Informationsasymmetrie erfordert es, qualitative Stufen zur Messung der Eintrittswahrscheinlichkeit eines Vorfalls einzuführen.

Es liegt in der Verantwortung eines jeden Sektors, seine eigenen realistischen Wahrscheinlichkeitsniveaus zu definieren und festzulegen.

Ein Beispiel für eine Wahrscheinlichkeitsskala und ihre Stufen ist in A.2 dargestellt.

6.3.8 Integration der Angreiferperspektive: Bewertung des Angriffspotentials

Wurde das Risikoniveau für ein bestimmtes Risikoszenario anhand der Wahrscheinlichkeit und der Folgen definiert, könnte jeder dieser Faktoren auf der Grundlage von Informationen zum Angriffspotential aktualisiert werden. Betrachtet man den Einfluss des Angriffspotentials auf die Wahrscheinlichkeit, so ist es schwer, diesen zuverlässig zu bewerten. Nehmen wir zum Beispiel ein sektorales IKT-System mit einem bestimmten Risiko, einer vorgegebenen Wahrscheinlichkeit und einem staatlich geförderten Akteur, der motiviert ist, anzugreifen. Es wäre schwer einzuschätzen, ob die Anwesenheit eines fähigen, motivierten Angreifers die Wahrscheinlichkeit, dass ein Risiko sich materialisiert, verdoppelt, verdreifacht oder vervierfacht.

Um die Informationen zum Angriffspotential mit den qualitativen Folgestufen und Risikobereichen zu kombinieren, muss der Risikoeigentümer stattdessen für jeden Angreifertyp evaluieren, ob dieser über die Motivation für einen Angriff auf ein sektorales System verfügt, und bestimmen, wie die üblichen Ziele des Angreifers sich auf die identifizierten Risikobereiche (sowie potentiellen Zusatzbereiche des Sektors) auswirken könnten. In derartigen Situationen sollte der Risikoeigentümer überlegen, ob das Risikoniveau für einen bestimmten Risikobereich erhöht werden sollte, um der Anwesenheit eines motivierten, fähigen Angreifers Rechnung zu tragen. Auf diese Weise werden die dazugehörigen Schutzanforderungen, die als Reaktion auf das bewertete Risiko anzuwenden sind, erhöht.

Die Risikobewertung jedweden Risikoszenarios, das IKT-Produkte oder IKT-Dienstleistungen oder IKT-Prozesse umfasst, kann eine Einschätzung des Angriffspotentials beinhalten, die auf einer qualitativen Skala basiert, die den Einfluss jedes dazugehörigen Faktors bestimmt.

Detaillierte Informationen zur Einschätzung des Angriffspotentials finden sich unter B.5. Eine Risikobewertung, die die Angreiferperspektive berücksichtigt, sollte die folgenden Schritte beinhalten:

- 1) Um eine vollständige Liste der Angreifertypen zu erhalten, werden sektorale Informationen zu Cyberbedrohungen (CTI) gesammelt, die sich mit der Motivation des Angreifers befassen. Informationen zu Bewertung, Zielen und bisherigen Angriffszielen werden genutzt, um einen Wert für das Angriffspotential dieses Angreifertyps abzuleiten. Auf Grundlage dieser Informationen entscheiden die sektoralen Stakeholder, ob ein Angreifertyp als relevanter Bedrohungsakteur für ein sektorales System erachtet wird. Die ausgewählten Angreifertypen werden dann einer weiteren Bewertung unterzogen.
- 2) Anhand der Liste relevanter Angreifertypen werden Bedrohungsinformationen zusammengestellt, die bisherige Angriffe und Kampagnen, den genutzten Angriffsvektor und Ansatz sowie die eingesetzten Mittel für jede Gefährdung und jeden Angreifer dieses Angreifertyps aufführen. Eine Analyse je spezifischer Gruppe von Bedrohungsakteuren innerhalb eines Angreiferstyps ist nicht erforderlich, da davon ausgegangen wer-

den kann, dass die Fähigkeiten und Gelegenheiten eines Typs auch für eine andere Bedrohungsgruppe des gleichen Typs verfügbar wären. Die gesammelten Daten sollten eine Zeitspanne von mehreren Jahren umfassen, um Verzerrungen aufgrund individueller Kampagnen und voreingenommener Berichte zu vermeiden und es den sektoralen Stakeholdern zu ermöglichen, nicht nur aktuelle Fähigkeiten und Gelegenheiten zu bewerten, sondern auch Extrapolationen für die nahe Zukunft vorzunehmen. Die Extrapolation sollte die voraussichtliche Entwicklung des Angriffspotentials bis zur nächsten Risikobewertung beurteilen sowie die Durchführung einer erneuten Bewertung und eine Aktualisierung.

- 3) Alle Berichte in Verbindung mit den Bedrohungsakteuren eines bestimmten Angreifertyps werden analysiert und die Merkmale dieses allgemeinen Angreifertyps hinsichtlich der Kriterien und ihrer Werte, wie in Anhang B diskutiert, ausgewertet. Die Anwendung der Merkmale ergibt den Wert des Angriffspotentials.
- 4) Das Ergebnis sind aggregierte Werte zum Angriffspotential für die drei Merkmale Gelegenheit, Mittel und Motiv, die mithilfe der in Anhang B diskutierten Vorgehensweise weiter zusammengefasst werden können, um ein allgemeines Angriffspotential für diesen bestimmten Angreifertyp zu bestimmen.

6.3.9 Erneute Risikobewertung für unterstützende Werte

Risikoszenarien werden im Hinblick auf Primärwerte identifiziert. Wie unter 6.3.4 ausgeführt, spielen unterstützende Werte im Geschäftsprozess beziehungsweise im System oder Prozess, das/der den Geschäftsprozess unterstützt, eine besondere Rolle.

Die erneute Bewertung ist ein notwendiger Schritt, um die speziellen Cybersecurity- und Vertrauenswürdigkeitsanforderungen für die bestimmungsgemäße Nutzung eines bestimmten IKT-Produkts oder IKT-Prozesses zu identifizieren.

Die Technologie des unterstützenden Werts ist ein weiterer Faktor, der für die Durchführung möglicher Angriffe relevant ist – wie die Betriebsumgebung – und somit für die Identifizierung relevanter Angreifertypen. Sie sollte deshalb einen weiteren Parameter darstellen, der für die erneute Bewertung der relevanten Angreifertypen und ihr spezielles Angriffspotential genutzt wird.

Die erneute Risikobewertung sollte eine detailliertere Bewertung möglicher Angriffswege und Angriffspotentiale im Hinblick auf bestimmte unterstützende Werte beinhalten. Sie kann das vorher bestimmte Risiko für einen relevanten Primärwert ändern.

Die erneute Risikobewertung für unterstützende Werte sollte in den folgenden Schritten durchgeführt werden:

- 1) Der Kontext für die Bewertung des unterstützenden Werts sollte dokumentiert werden. Dies beinhaltet die bestimmungsgemäße Nutzung, die Betriebsumgebung und die Technologie des unterstützenden Werts. Des Weiteren sollte dokumentiert werden, ob Geschäftsanforderungen vorhanden sind, die – unabhängig von den risiko- oder angreiferbasierten Überlegungen – Auswirkungen auf Cybersecurity-, Vertrauenswürdigkeits- oder Zertifizierungsanforderungen des unterstützenden Werts haben könnten. Dies kann beispielsweise bei relevanten Vorschriften staatlicher Behörden der Fall sein.
- 2) Die Liste der im Bezug auf die relevanten Risikoszenarien maßgeblichen Angreifertypen und ihrer Angriffspotentiale sollte im Hinblick auf die spezielle Technologie und die Betriebsumgebung des unterstützenden Werts hin überprüft werden. Jegliche Änderungen im Hinblick auf die relevantesten Angreifertypen, ihr Angriffspotential und ihre Motivation sollten dokumentiert werden. Der revidierte Wert sollte für die erneute Risikobewertung verwendet werden.
- 3) Sollten während des vorherigen Schritts Änderungen beim Wahrscheinlichkeitsniveau der relevanten Risikoszenarien auftreten, sollte das mit dem Wert verbundene Risiko neu beurteilt werden. Der revidierte Wert sollte dem unterstützenden Wert zugeordnet und im Rahmen weiterer Schritte zur Definition seiner Cybersecurity- und Vertrauenswürdigkeitsanforderungen genutzt werden.

Beispiele zur Berechnung des Angriffspotentials sind in B.5 dargestellt.

7 Normalisierte Darstellung von Risiko, Cybersecurity und Vertrauenswürdigkeit

7.1 Ergebnisse von Risikobewertungen: Meta-Risikoklassen

Um einen einheitlichen Zertifizierungsansatz bereitzustellen und sicherzustellen, dass Zertifikate im gesamten Sektor einheitlich und vergleichbar sind, ist es notwendig, die Überlegungen auf der Basis vergleichbarer, für den Sektor geeigneter Risikoniveaus anzustellen, die als „Meta-Risikoklassen“ (MRC) bezeichnet werden.

Sektorale Risikobewertungen sollten von der koordinierenden Einheit des Sektors oder dem Entwickler eines sektoralen Cybersecurity-Zertifizierungsprogramms auf einer übergeordneten Ebene durchgeführt werden. Beide sollten die relevanten Stakeholder-Rollen direkt aus dem Sektor und die dazugehörigen Organisationen involvieren, die als Risikoeigentümer betrachtet werden sollten:

- die Stakeholder und die koordinierende Einheit, die an der Bereitstellung der sektoralen Dienstleistungen beteiligt sind („geschäftliche Risikoeigentümer“);
- Konsumenten der sektoralen Dienstleistungen;
- die Gesellschaft insgesamt, sowohl auf europäischer als auch auf internationaler Ebene;
- staatliche Risikoeigentümer.

Die in der sektoralen Risikobewertung ausgewählten Kriterien werden auf alle qualitativen Stufen von Wahrscheinlichkeit und Folgen angewendet und es wird eine Formel für die Risikoeinschätzung vorgegeben, um qualitative Risikoniveaus zu erzielen, die mithilfe von Namen oder Farben dargestellt werden.

Ein Beispiel für Meta-Risikoklassen ist in A.3 dargestellt.

7.2 Risikobasierte Definition von allgemeinen Sicherheitsstufen und Auswahl von Sicherheitsmaßnahmen

7.2.1 Allgemeines

In sektoralen Systemen werden Cybersecurity- und Vertrauenswürdigkeitsanforderungen für unterstützende Werte so gewählt, dass sie dem Angriffspotential entsprechen. So wird sichergestellt, dass die spezifizierte Sicherheitsstufe ausreichend ist, um einen Schutz gegen die jeweilige Angriffsstufe zu bieten, wobei die Stringenz und die Tiefe der Bewertung die Fähigkeiten des Angreifertyps widerspiegeln. Cybersicherheitsanforderungen und Sicherheitsmaßnahmen sollten zudem je Vertrauenswürdigkeitsstufe dokumentiert werden (siehe 0). Diese Kombination von Anforderungen sorgt dafür, dass Cybersicherheit und die Einführung von Sicherheitsstufen zu einem programmübergreifenden Konsistenzmerkmal werden.

BEISPIEL Die Cybersicherheitsanforderungen für industrielle Datendiodeen könnten sehr einfach sein, doch das Risiko, sensible Informationen preiszugeben, ist nach wie vor sehr hoch und sollte deshalb mit einer geeigneten Vertrauenswürdigkeitsstufe einhergehen.

Die vorausgehenden Überlegungen führen zu der Schlussfolgerung, dass eine Struktur von allgemeinen Sicherheitsstufen (CSL) etabliert werden sollte, die den unter 7.1 definierten Meta-Risikoklassen entspricht.

Die Verfügbarkeit von CTI bietet die Möglichkeit, Informationen zu Angreifern zu berücksichtigen. Auf diese Weise sollten relevante Angriffspotentiale als Beitrag zur Einschätzung des erforderlichen Sicherheitsniveaus berücksichtigt werden.

Da die sektorale Risikobewertung mit ISO/IEC 27005 übereinstimmen sollte, sollten in den folgenden Unterabschnitten verwendete Definitionen und Terminologie zu Cybersicherheit und CSL [4] folgen. Es kann jedoch auch jeder andere Katalog mit Sicherheitsmaßnahmen verwendet werden, um eine Auswahl an Sicherheitsmaßnahmen anzulegen, insbesondere im Kontext spezieller sektoraler Anforderungen.

7.2.2 Einführung von allgemeinen Sicherheitsstufen (CSL)

Die Kohärenz zwischen Cybersecurity-Zertifizierungsprogrammen erfordert einen allgemeinen Ansatz bei den Sicherheitsstufen. Zudem müssen die Sicherheitsstufen den Risikoniveaus, den Angriffspotentialen und, wenn auch indirekt, den Vertrauenswürdigkeitsstufen entsprechen.

Die Informationen zu Risiken und die damit verbundene MRC unterstützen die Definition der erforderlichen CSL und dazugehöriger Sicherheitsmaßnahmen, so dass diese das Risiko effizient und wirksam mindern können.

Ein Beispiel für eine Klassifizierung von allgemeinen Sicherheitsstufen (CSL) ist in A.4 dargestellt.

Die Verbindung mit dem Parameter Angriffspotential (APL), der durch die CTI bestimmt wird, ermöglicht es, zu prüfen, ob die gewählte CSL die Kraft hat, dem angenommenen Angriffspotential zu widerstehen.

Die Beziehung sollte wie folgt abgebildet werden:

CSL_x – eine definierte Reihe von Maßnahmenzielen und Maßnahmen mindert das Risiko auf der Ebene → MRC_x
und bietet einen Schutz gegen Angreifer mit einem Angriffspotential unter → APL_x

In beiden Fällen besteht standardmäßig eine direkte Beziehung zwischen den gleichen Ebenen der Parameter MRC und CSL, sowie zwischen APL und CSL. Sektorale Stakeholder dürfen während des sektoralen Assessments jedoch von dieser Standardbeziehung abweichen.

7.2.3 Einsatz von Meta-Risikoklassen und allgemeinen Sicherheitsstufen zur sektoralen Risikobehandlung

Während der sektoralen Risikobewertung sollten jedwede identifizierte Risiken einer Meta-Risikoklasse zugeordnet werden. In einem zweiten Schritt sollte eine feste Expertengruppe etabliert werden, um Maßnahmenziele zur Risikominderung zu definieren. Diese Maßnahmenziele übernehmen die zugeordneten MRC als Parameter:

Die möglichen Sicherheitsmaßnahmen stehen in direkter Relation zu den gewählten MRC (siehe 7.1). Die Expertengruppe sollte aus den möglichen Maßnahmen für jede angewandte MRC die geeigneten Sicherheitsmaßnahmen zur Risikobehandlung auswählen.

In einigen Fällen gibt es keine Maßnahme, die die erforderliche CSL unterstützt. In dem Fall sollten Maßnahmen oder eine Kombination von Maßnahmen oder eine Maßnahme, die der erforderlichen CSL so nah wie möglich kommt, angewendet werden.

7.2.4 Angriffspotential als Kriterium für die Auswahl der CSL von Maßnahmen

Es ist ein fundamentaler Grundsatz, dass Maßnahmen den angenommenen Angreifertypen und ihren Fähigkeiten widerstehen sollten.

Beispiele für CSL-Anwendungen, die die unterschiedlichen Angriffspotentiale berücksichtigen, sind in Anhang C enthalten.

Die Bewertung kann zur Zuordnung einer niedrigeren MRC für das identifizierte Risiko führen als das relevante Angriffspotential. In einem solchen Fall sollte das CSL auf Basis des APL gewählt werden.

BEISPIEL Das Risiko eines unbefugten Zugriffs wird als „mittel“ eingeschätzt und das Angriffspotential wird als „hoch“ eingeschätzt. Maßnahmen wie der „Einsatz von Passwörtern“ könnten den Angriff nicht wirksam abwehren. In solchen Fällen kann eine Multi-Faktor-Authentifizierung in Betracht gezogen werden.

Während des sektoralen Assessments können die sektoralen Stakeholder in speziellen Fällen von dieser Standardbeziehung abweichen. Derartige Abweichungen sollten begründet und dokumentiert werden.

7.3 Einheitliche Implementierung von Vertrauenswürdigkeit

7.3.1 Einführung

Das Ziel einer einheitlichen Implementierung von Vertrauenswürdigkeitsstufen sollte im Kontext der folgenden Treiber gesehen werden:

- 1) Eine einheitliche Implementierung von Schlüsselparametern wie Risiken im Zusammenhang mit einer bestimmungsgemäßen Nutzung, Cybersecurity- und Vertrauenswürdigkeitsstufen über Cybersecurity-Zertifizierungsprogramme hinweg verhindert eine Fragmentierung zwischen den Programmen und ermöglicht eine Wiederverwendung und Anerkennung von Zertifikaten durch den Markt.
- 2) Die Anforderungen für die Zertifizierung von IKT-Produkten, IKT-Prozessen und IKT-Dienstleistungen kann sich je nach Technologien, Zielmärkten, verantwortlichen Stakeholdern usw. unterscheiden. Zur Unterstützung dieser Anforderungen können spezielle Cybersecurity-Zertifizierungsprogramme etabliert werden. Ohne eine Harmonisierung der Maßnahmen könnten diese Abweichungen zu einer Fragmentierung zwischen den Programmen führen und eine Anerkennung von Zertifikaten eines Programms durch ein anderes Programm verhindern.

Zwischen diesen beiden Richtungen besteht offenbar ein Potential für Konflikte. Es muss deshalb ein Gleichgewicht zwischen dem Ziel der Anerkennung und Wiederverwendung von Zertifikaten und der erforderlichen Flexibilität bei der Implementierung der Programme hergestellt werden.

Das Konzept der allgemeinen Vertrauenswürdigkeitsreferenz, das in den folgenden Abschnitten beschrieben wird, unterstützt die Herstellung eines solchen Gleichgewichts.

Die Vertrauenswürdigkeitsreferenz sollte auf bewährten, vertrauenswürdigen Standards und Methoden basieren.

7.3.2 Definition eines allgemeinen Vertrauenswürdigkeitsreferenzkonzepts basierend auf ISO/IEC 15408

ISO/IEC 15408-3 spezifiziert die Anfälligkeitsanalyse auf der Basis einer Definition von AVA_VAN-Vertrauenswürdigkeitskomponenten. Diese haben 5 Ebenen von zunehmender Stringenz und Tiefe. Die Evaluierungsmethoden für die AVA_VAN-Vertrauenswürdigkeitskomponenten sind klar definiert, vom europäischen und internationalen Markt anerkannt und in einer Vielzahl von Evaluierungseinrichtungen weltweit implementiert. Es sollte an dieser Stelle angemerkt werden, dass AVA_VAN-basierte Konzepte auch von einigen brancheneigenen Cybersecurity-Zertifizierungsprogrammen genutzt werden. Auch wenn diese nicht immer völlig mit ISO/IEC 15408 übereinstimmen, nutzen sie das AVA_VAN-Konzept, um von seinen bewährten Evaluierungsmethoden zu profitieren.

Die Bestimmung des Angriffspotentials für einen Angriff entspricht der Identifizierung des Aufwands, der erforderlich ist, um den Angriff zu erzeugen und nachzuweisen, dass er erfolgreich auf ein bestimmtes Objekt angewendet werden kann, wodurch die Anfälligkeit im Objekt ausgenutzt wird.

Die folgenden Faktoren sollten bei der Analyse des Angriffspotentials, das zur Ausnutzung einer Anfälligkeit erforderlich ist, berücksichtigt werden:

- a) Zeit, die zur Identifizierung und Ausnutzung benötigt wird (**Abgelaufene Zeit**);
- b) Erforderliche spezielle Sachkenntnis (**Fachwissen**);
- c) Wissen über das Design und den Betrieb des Objekts (**Wissen über das anvisierte Objekt**);
- d) **Zugriffsgelegenheit**;

e) **IT-Hardware/Software oder andere Geräte**, die für die Ausnutzung erforderlich sind.

Eine detaillierte Beschreibung zur Berechnung des Angriffspotentials und zur Zuordnung der verschiedenen Stufen des Angriffspotentials sind in ISO/IEC 18045, B.4 zu finden.

Um Abweichungen von den strengen Definitionen der AVA_VAN-Vertrauenswürdigkeitskomponenten in ISO/IEC 15408 zu ermöglichen, wird die Einführung des Begriffs „allgemeine Vertrauenswürdigkeitsreferenz“ (CAR) vorgeschlagen. Dieses Konzept ist in Tabelle 1 dargestellt.

Tabelle 1 — Zuordnung der allgemeinen Vertrauenswürdigkeitsreferenz (CAR)

Allgemeine Vertrauenswürdigkeitsreferenz (CAR)	Assoziierte Bezugsinhalte für die AVA_VAN-Vertrauenswürdigkeitskomponenten nach ISO/IEC 15408-3	Entsprechendes Angriffspotential nach ISO/IEC 18045
1	AVA_VAN.1 Anfälligkeitsuntersuchung	niedrig
2	AVA_VAN.2 Anfälligkeitsanalyse	niedrig
3	AVA_VAN.3 Fokussierte Anfälligkeitsanalyse	zunehmend-niedrig
4	AVA_VAN.4 Methodische Anfälligkeitsanalyse	moderat
5	AVA_VAN.5 Erweiterte methodische Anfälligkeitsanalyse	hoch

Das Angriffspotential für den Angreifer kann als „mehr als hoch“ eingestuft werden (CAR5+). In diesem besonderen Fall sind bisher keine Evaluierungsmethoden für dieses Level verfügbar, da CAR5+ nicht über irgendeine in ISO/IEC 15408 definierte Vertrauenswürdigkeitskomponente abgebildet werden kann.

Bei der endgültigen Bestimmung des CAR sollten gesetzliche, behördliche oder vertragliche Anforderungen berücksichtigt werden.

Bei der Implementierung des CAR-Konzepts im Rahmen des Programms sollte die Frage beantwortet werden, wie die gewünschte Vertrauenswürdigkeitsstufe für die im Programm beinhalteten IKT-Produkte/IKT-Prozesse/IKT-Dienstleistungen definiert und gemessen werden kann.

Wie in ISO/IEC 15408 kann ein auf dem Angriffspotential basierender Ansatz (siehe 7.2.4) zur Beantwortung der Frage herangezogen werden, wie im nächsten Abschnitt beschrieben.

7.3.3 Anwendung des CTI-Konzepts zum Angriffspotential auf CAR

Der Parameter „Angriffspotential“, der in ISO/IEC 18045 ausführlich beschrieben und zum Zweck der Produktevaluierung genutzt wurde, dient als Beispiel und Ausgangspunkt für Überlegungen zu einer breiteren Definition des Parameters, basierend auf dem Kontext der CTI.

Der Unterschied zwischen einem CTI- und einem ISO/IEC 18045-basierten Ansatz beim Angriffspotential liegt im Faktor „Motivation“. Er ermöglicht die Einführung der Angreiferperspektive in die Bewertung der Primärwerte, nicht nur der unterstützenden Werte (siehe Bild 4).

Darüber hinaus nimmt der CTI zur Unterstützung der Risikobewertung die Sicht des Angreifers ein, indem die Motivation des Angreifers beim Angriff auf bestimmte Informations- oder andere Primärwerte eingebracht wird. Zudem sollte auch die Stärke des Angriffspotentials bei der Bewertung von Cybersicherheitsrisiken für unterstützende Werte berücksichtigt werden und, ausgehend vom Ergebnis, werden die Cybersecurity- und Vertrauenswürdigkeitsanforderungen etabliert.

ISO/IEC 18045 bewertet aus Sicht des Evaluierenden, ob ein unterstützender Wert (als Evaluierungsgegenstand bezeichnet) ausreichend gegen ein bestimmtes Angriffspotential gewappnet ist.

Es ist wichtig, dass die Methode vergleichbare Ergebnisse für den unterstützenden Wert hervorbringt, damit der Evaluierende bestätigen kann, dass die zugewiesenen Cybersecurity- und Vertrauenswürdigkeitsanforderungen in beiden Fällen erfüllt werden.

Ein Beispiel für eine CTI-basierte Zuordnung des Angriffspotentials ist in B.5.5 dargestellt.

Ein Beispiel für MRC, APL und die resultierende CAR ist in A.5 dargestellt.

8 Zuordnung von Cybersecurity- und Vertrauenswürdigkeitsanforderungen zur Programmdarstellung

Das sektorale Cybersecurity Assessment nutzt normalisierte Darstellungen für Risikoklassen (MRC), Cybersecurity- (CSL) und Vertrauenswürdigkeitsanforderungen (CAR), die für die unterstützenden Werte gelten. Cybersecurity-Zertifizierungsprogramme haben jedoch üblicherweise ihre eigenen Merkmale zur Darstellung von Cybersicherheits- und Vertrauenswürdigkeitsstufen sowie Sicherheitszielen. Aus diesem Grund sollten die anhand von CAR und CSL dokumentierten Ergebnisse des sektoralen Cybersecurity Assessments der Darstellung des bestehenden oder geplanten Cybersecurity-Zertifizierungsprogramms zugeordnet werden.

Die CSL sollten den Sicherheitszielen oder jedweder anderen Darstellung der für das Programm etablierten, übergeordneten Cybersicherheitsanforderungen zugeordnet werden.

Für die CAR lässt sich die Zuordnung sehr einfach umsetzen, vorausgesetzt die Programmdefinition der Vertrauenswürdigkeitsstufen nimmt Bezug auf die AVA_VAN-Komponenten, wie unter 7.3.2 diskutiert und in Tabelle 1 dargestellt.

Sollte dies nicht der Fall sein, besteht die Möglichkeit, die Widerstandsfähigkeit gegen ein bestimmtes Angriffspotential (APL) einzuschätzen, die die Evaluierungsmethode des Programms für seine speziellen Vertrauenswürdigkeitsstufen bestätigen kann. Sobald die Definitionen der Vertrauenswürdigkeitsstufen des Programms mit einem bestimmten APL assoziiert sind, können die dazugehörigen CAR durch die unter 7.7.3 vorgegebene Beziehung zwischen APL und AVA_VAN definiert werden.

Anhang D bietet ein Beispiel einer derartigen Darstellung für [5].

Anhang A (informativ)

Beispiele für normalisierte Skalen bei der sektoralen Risikobewertung

A.1 Qualitativer Ansatz zur Bewertung der Folgen

In einem Ansatz werden generische Folgenstufen zur Verwendung bei sektoralen Risikobewertungen definiert. Diese Stufen, Wirkungsklassen (IC, en: impact classes) genannt, messen auf qualitative Weise den Schaden des Risikoszenarios auf das Geschäft der Stakeholder. Die definierten Wirkungsklassen sind in Tabelle A.1 angegeben.

Tabelle A.1 — Wirkungsklassen — Beispiel 1

IC1	IC2	IC3	IC4	IC5
vernachlässigbare Auswirkungen	geringfügige Auswirkungen	mittelschwere Auswirkungen	schwerwiegende Auswirkungen	katastrophale Auswirkungen

Der Stakeholder kann die qualitativen Stufen selbstverständlich in quantitative übertragen.

BEISPIEL Eine schwerwiegende Auswirkung könnte ein 10%-iger Umsatzverlust aufgrund eines Vertragsbruches oder ein Verlust von 15 % der Kunden aufgrund eines Vertrauensverlustes sein.

Die Bewertung der Folgen kann durch die Einführung von Risikobereichen erweitert werden. Risikobereiche können sowohl für ein Risikoszenario als auch für Stakeholder unterschiedlich sein. Ein Beispiel dafür, wie Risikobereiche und Folgenskala die Bewertung der Auswirkungen für einen bestimmten Risikobereich widerspiegeln, ist in Tabelle A.2 angegeben.

ANMERKUNG Im Kontext von Tabelle A.2 werden die Begriffe „Auswirkung“ und „Wirkung“ synonym verwendet.

Tabelle A.2 — Wirkungsklassen je Risikobereich — Beispiel 2

Risikobereich	IC1	IC2	IC3	IC4	IC5
1. Auswirkung auf Geschäftsbetrieb und Funktionalität	begrenzte Wirkung auf eine Organisation	signifikante Wirkung auf eine Organisation	begrenzte Wirkung auf mehrere Entitäten eines Sektors oder signifikante Wirkung auf wenige Entitäten eines Sektors	signifikante Wirkung auf mehrere Entitäten innerhalb einiger weniger Sektoren oder signifikante Wirkung auf wenige Entitäten innerhalb mehrerer Sektoren	Störung eines gesamten Sektors und/oder signifikante Wirkung auf das Geschäft, die Wirtschaft und die Gesellschaft als Ganzes
2. Auswirkung auf Bürger (z. B. Unvermögen, die erwartete Serviceverfügbarkeit sicherzustellen)	geringe Auswirkung auf den Alltag der Bürger		starke Auswirkung auf den Alltag der Bürger	gravierende Auswirkung auf den Alltag der Bürger	
3. Wirkung in Übereinstimmung mit den verarbeiteten Daten	sektorales geistiges Eigentum	personenbezogene Daten	besondere Kategorien personenbezogener Daten	für kritische Infrastrukturen wesentliche Daten	Daten, die die nationale Sicherheit betreffen
4. Auswirkung auf Reputation und Vertrauen	geringfügige Rufschädigung einiger weniger Organisationen	geringfügige Rufschädigung vieler Organisationen und/oder des Sektors	schwerwiegende Rufschädigung vieler Organisationen und/oder des Sektors	schwerwiegende Rufschädigung des gesamten Sektors und/oder Beschädigung des Vertrauens in eine bestimmte Technologie oder Dienstleistung(en)	schwerwiegende Rufschädigung von mehr als einem Sektor und/oder Vertrauensverlust einer bestimmten Technologie oder Dienstleistung(en)

Tabelle A.2 (fortgesetzt)

Risikobereich	IC1	IC2	IC3	IC4	IC5
5. Auswirkung auf Vertragsanforderungen	geringfügige Nicht-Einhaltung vertraglicher Anforderungen		schwerwiegende Nicht-Einhaltung vertraglicher Anforderungen		
6. Auswirkung auf Gesundheit und Leben			negative gesundheitliche Auswirkungen für Menschen und/oder Umwelt, die nicht behebbar sind	lebensverändernde gesundheitliche Folgen und/oder Umweltschädigungen	potentielle Verluste von Menschenleben und/oder Umweltschädigungen

A.2 Qualitativer Ansatz zur Wahrscheinlichkeitsbewertung

Ein Beispiel für eine Wahrscheinlichkeitsbewertung mit fünf Stufen ist in Tabelle A.3 dargestellt.

Tabelle A.3 — Wahrscheinlichkeitsbewertung — ein Beispiel

L1	L2	L3	L4	L5
Eintreten des Risikoszenarios ist sehr unwahrscheinlich	Eintreten des Risikoszenarios ist unwahrscheinlich	Eintreten des Risikoszenarios ist möglich	Eintreten des Risikoszenarios ist sehr wahrscheinlich	Eintreten des Risikoszenarios ist fast sicher

A.3 Qualitativer Ansatz zur Risikoeinschätzung

Qualitative Ansätze zur Risikoeinschätzung beinhalten eine Formel, die Informationen zu Folgen und Wahrscheinlichkeit zusammenführt. Qualitative Risikoniveaus können in Abhängigkeit von Wahrscheinlichkeitsstufen ausgedrückt werden (siehe Tabelle A.1 oder Tabelle A.2 und Folgen (siehe Tabelle A.3). Das Ergebnis sind 5 abgestufte Meta-Risikoklassen (MRC), siehe Tabelle A.4.

Tabelle A.4 — Meta-Risikoklassen — Beispiel

	Wahrscheinlichkeitsstufen				
Wirkungsklasse	L1	L2	L3	L4	L5
IC5	MRC4	MRC5	MRC5	MRC5	MRC5
IC4	MRC3	MRC3	MRC4	MRC4	MRC5
IC3	MRC2	MRC2	MRC3	MRC3	MRC4
IC2	MRC1	MRC1	MRC2	MRC3	MRC3
IC1	MRC1	MRC1	MRC1	MRC2	MRC3

Die Skala mit den fünf Meta-Risikoklassen kann anhand der folgenden Beschreibungen in einer weithin anerkannten, farbgestützten Risikoklassifizierung ausgedrückt werden: