

DIN EN ISO/IEC 15408-1



ICS 35.030

Entwurf

Einsprüche bis 2020-07-08
Vorgesehen als Ersatz für
die 2011-03 zurückgezogene
Norm
DIN ISO/IEC 15408-1:2007-11;
Ersatz für
E DIN EN ISO/IEC 15408-1:2020-01

**Informationstechnik –
IT-Sicherheitsverfahren –
Evaluationskriterien für IT-Sicherheit –
Teil 1: Einführung und allgemeines Modell (ISO/IEC 15408-1:2009);
Deutsche und Englische Fassung prEN ISO/IEC 15408-1:2019**

Information technology –
Security techniques –
Evaluation criteria for IT security –
Part 1: Introduction and general model (ISO/IEC 15408-1:2009);
German and English version prEN ISO/IEC 15408-1:2019

Technologies de l'information –
Techniques de sécurité –
Critères d'évaluation pour la sécurité TI –
Partie 1: Introduction et modèle général (ISO/IEC 15408-1:2009);
Version allemande et anglaise prEN ISO/IEC 15408-1:2019

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2020-05-08 wird der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt.

Weil die beabsichtigte Norm 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 Saatwinkler Damm 42/43, 13627 Berlin.

Die Empfänger dieses Norm-Entwurfs werden gebeten, mit ihren Kommentaren jegliche relevanten Patentrechte, die sie kennen, mitzuteilen und unterstützende Dokumentationen zur Verfügung zu stellen.

Gesamtumfang 152 Seiten

DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)

Nationales Vorwort

Der Text von ISO/IEC 15408-1:2009 wurde vom Technischen Komitee ISO/IEC JTC 1 „Information technology“ der Internationalen Organisation für Normung (ISO) erarbeitet und als prEN ISO/IEC 15408-1:2019 durch das Technische Komitee CEN/CLC/JTC 13 „Cybersicherheit und Datenschutz“ übernommen, dessen Sekretariat von DIN (Deutschland) gehalten wird.

Das zuständige nationale Gremium ist der Arbeitskreis NA 043-01-27-03 AK „Evaluationskriterien für IT-Sicherheit“ 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/IEC 27001	siehe	DIN EN ISO/IEC 27001
ISO/IEC 27002	siehe	DIN EN ISO/IEC 27002

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

Änderungen

Gegenüber der 2011-03 zurückgezogenen Norm DIN ISO/IEC 15408-1:2007-11 wurden folgende Änderungen vorgenommen:

- a) redaktionelle Korrekturen;
- b) Abschnitt 3: Korrektur der Begriffe „Sicherheitsproblem“ und „Sicherheitsdomänen“;
- c) Abschnitt 8.3: Erklärung der strikten Konformität, Streichung der früheren Abbildung 4.

Nationaler Anhang NA (informativ)

Literaturhinweise

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

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

Informationstechnik — IT-Sicherheitsverfahren - Evaluationskriterien für IT-Sicherheit — Teil 1: Einführung und allgemeines Modell (ISO/IEC 15408-1:2009)

Technologies de l'information — Techniques de sécurité - Critères d'évaluation pour la sécurité TI — Partie 1 : Introduction et modèle général (ISO/IEC 15408-1:2009)

Information technology — Security techniques - Evaluation criteria for IT security — Part 1: Introduction and general model (ISO/IEC 15408-1:2009)

ICS:

Deskriptoren

Dokument-Typ: Europäische Norm
Dokument-Untertyp:
Dokument-Stage: CEN-Umfrage
Dokument-Sprache: D

STD Version 2.10b

Inhalt

	Seite
Europäisches Vorwort	5
Vorwort	6
Einleitung	7
1 Anwendungsbereich	9
2 Normative Verweisungen	9
3 Begriffe	9
3.1 In ISO/IEC 15408 verwendete Begriffe	9
3.2 Begriffe in Zusammenhang mit der Klasse ADV	18
3.3 Begriffe in Zusammenhang mit der Klasse AGD	22
3.4 Begriffe in Zusammenhang mit der Klasse ALC	23
3.5 Begriffe in Zusammenhang mit der Klasse AVA	27
3.6 Begriffe in Zusammenhang mit der Klasse ACO	27
4 Symbole und Abkürzungen	28
5 Übersicht	29
5.1 Allgemein	29
5.2 Der Evaluierungsgegenstand (TOE)	29
5.2.1 Unterschiedliche Darstellungen des TOEs	30
5.2.2 Unterschiedliche Konfigurationen des TOEs	30
5.3 Zielgruppe der ISO/IEC 15408	31
5.3.1 Verbraucher	31
5.3.2 Entwickler	31
5.3.3 Evaluatoren	31
5.3.4 Weitere	31
5.4 Die verschiedenen Teile der ISO/IEC 15408	32
5.5 Evaluierungskontext	33
6 Allgemeines Modell	33
6.1 Einführung in das allgemeine Modell	33
6.2 Vermögenswerte und Gegenmaßnahmen	34
6.2.1 Angemessenheit der Gegenmaßnahmen	36
6.2.2 Korrektheit des TOEs	37
6.2.3 Korrektheit der Betriebsumgebung	38
6.3 Evaluierung	38
7 Anpassung von Sicherheitsanforderungen	39
7.1 Operationen	39
7.1.1 Die Operation Iteration	40
7.1.2 Die Operation Zuweisung	40
7.1.3 Die Operation Auswahl	41
7.1.4 Die Operation Präzisierung	41
7.2 Abhängigkeiten zwischen Komponenten	42
7.3 Erweiterte Komponenten	42
8 Schutzprofile und Pakete	43
8.1 Einleitung	43
8.2 Pakete	43

8.3	Schutzprofile	43
8.4	Verwendung von PPs und Paketen	46
8.5	Verwendung mehrerer Schutzprofile	46
9	Evaluierungsergebnisse	47
9.1	Einleitung	47
9.2	Ergebnisse einer PP-Evaluierung	48
9.3	Ergebnisse einer ST-/TOE-Evaluierung	48
9.4	Konformitätsanspruch	48
9.5	Verwendung der ST-/TOE-Evaluierungsergebnisse	49
Anhang A (informativ) Spezifikation von Sicherheitsvorgaben		50
A.1	Ziel und Aufbau dieses Anhangs	50
A.2	Verpflichtender Inhalt einer ST	50
A.3	Verwendung einer ST	51
A.3.1	Wie eine ST verwendet werden sollte	51
A.3.2	Wie eine ST nicht verwendet werden sollte	52
A.4	ST-Einleitung (ASE_INT)	52
A.4.1	ST-Verweisung und TOE-Verweisung	52
A.4.2	TOE-Überblick	53
A.4.3	TOE-Beschreibung	54
A.5	Konformitätsansprüche (ASE_CCL)	55
A.6	Sicherheitsproblemdefinition (ASE_SPD)	55
A.6.1	Einleitung	55
A.6.2	Bedrohungen	55
A.6.3	Organisatorische Sicherheitspolitik (OSP)	56
A.6.4	Annahmen	56
A.7	Sicherheitszielsetzungen (ASE_OBJ)	57
A.7.1	Allgemeine Lösung	57
A.7.2	Teillösungen	58
A.7.3	Beziehung zwischen Sicherheitszielsetzungen und Sicherheitsproblemdefinition	59
A.7.4	Sicherheitszielsetzungen: Schlussfolgerung	60
A.8	Erweiterte Komponentendefinition (ASE_ECD)	60
A.9	Sicherheitsanforderungen (ASE_REQ)	61
A.9.1	Sicherheitsfunktionsanforderungen (SFRs)	61
A.9.2	Vertrauenswürdigkeitsanforderungen (SARs)	63
A.9.3	SARs und die Begründung der Sicherheitsanforderungen	63
A.9.4	Sicherheitsanforderungen: Schlussfolgerung	63
A.10	Zusammenfassende Spezifikation des TOEs (ASE_TSS)	64
A.11	Fragen, die mit einer ST beantwortet werden können	64
A.12	Sicherheitsvorgaben mit niedriger Vertrauenswürdigkeit	65
A.13	Verweisen auf andere Normen in einer ST	67
Anhang B (informativ) Spezifikation von Schutzprofilen		68
B.1	Ziel und Aufbau dieses Anhangs	68
B.2	Verpflichtender Inhalt eines PPs	68
B.3	Verwendung eines PPs	69
B.3.1	Wie ein PP verwendet werden sollte	69
B.3.2	Wie ein PP nicht verwendet werden sollte	70
B.4	PP-Einleitung (APE_INT)	70
B.4.1	PP-Verweisung	70
B.4.2	TOE-Überblick	70
B.5	Konformitätsansprüche (APE_CCL)	71
B.6	Sicherheitsproblemdefinition (APE_SPD)	72
B.7	Sicherheitszielsetzungen (APE_OBJ)	72
B.8	Erweiterte Komponentendefinition (APE_ECD)	72
B.9	Sicherheitsanforderungen (APE_REQ)	72

B.10	Zusammenfassende Spezifikation des TOEs.....	72
B.11	Schutzprofile mit niedriger Vertrauenswürdigkeit.....	72
B.12	Verweisen auf andere Normen in einem PP	73
Anhang C (informativ) Leitlinien für Operationen.....		74
C.1	Einleitung	74
C.2	Beispiele für Operationen	74
C.2.1	Die Operation Iteration	74
C.2.2	Die Operation Zuweisung	74
C.2.3	Die Operation Auswahl.....	74
C.2.4	Die Operation Präzisierung	75
C.3	Organisation von Komponenten	75
C.3.1	Klasse	76
C.3.2	Familie	76
C.3.3	Komponente	76
C.3.4	Element.....	76
C.4	Erweiterte Komponenten	76
C.4.1	Wie erweiterte Komponenten definiert werden	76
Anhang D (informativ) PP-Konformität		78
D.1	Einleitung	78
D.2	Strikte Konformität.....	78
D.3	Nachweisliche Konformität	79
Literaturhinweise.....		80

Europäisches Vorwort

Der Text von ISO/IEC 15408-1:2009 wurde vom Technischen Komitee ISO/IEC JTC 1 „Information technology“ der Internationalen Organisation für Normung (ISO) und der Internationalen Elektrotechnischen Kommission (IEC) erarbeitet und als prEN ISO/IEC 15408-1:2020 durch das Technische Komitee CEN/CLC/JTC 13 „Cybersicherheit und Datenschutz“ übernommen, dessen Sekretariat von DIN gehalten wird.

Dieses Dokument ist derzeit zur CEN-Umfrage vorgelegt.

Anerkennungsnotiz

Der Text von ISO/IEC 15408-1:2009 wurde von CEN als prEN ISO/IEC 15408-1:2020 ohne irgendeine Abänderung genehmigt.

Vorwort

ISO (die Internationale Organisation für Normung) und IEC (die Internationale Elektrotechnische Kommission) bilden das auf die weltweite Normung spezialisierte System. Nationale Normungsorganisationen, die Mitglieder von ISO oder IEC sind, beteiligen sich an der Entwicklung von Internationalen Normen in Technischen Komitees, die von der jeweiligen Organisation eingerichtet wurden, um spezifische Gebiete technischer Aktivitäten zu behandeln. Auf Gebieten von beiderseitigem Interesse arbeiten die Technischen Komitees von ISO und IEC zusammen. Internationale Organisationen, staatlich und nicht-staatlich, in Liaison mit ISO und IEC, nehmen ebenfalls an der Arbeit teil. Auf dem Gebiet der Informationstechnologie haben ISO und IEC ein gemeinsames technisches Komitee (JTC, en: joint technical committee), ISO/IEC JTC 1, eingerichtet.

Internationale Normen werden in Übereinstimmung mit den Gestaltungsregeln der ISO/IEC-Direktiven, Teil 2 erarbeitet.

Die Hauptaufgabe der gemeinsamen Technischen Komitees besteht in dem Erarbeiten von Internationalen Normen. Die von den Technischen Komitees angenommenen Norm-Entwürfe werden den Mitgliedsorganisationen zur Umfrage zur Verfügung gestellt. Für eine Veröffentlichung als Internationale Norm wird eine Zustimmung von mindestens 75 % der Mitgliedsländer, die abgestimmt haben, benötigt.

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. ISO ist nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

ISO/IEC 15408-1 wurde vom gemeinsamen Technischen Komitee ISO/IEC JTC 1, *Information technology*, Unterkomitee SC 27, *IT Security technique*, erarbeitet. Der identische Text der ISO/IEC 15408 ist bei den am Common Criteria Project beteiligten Organisationen als Common Criteria for Information Technology Security Evaluation (Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik) veröffentlicht. Die einheitliche XML-Quelle für beide Veröffentlichungen findet sich unter <http://www.commoncriteriaportal.org/cc/>

Diese dritte Fassung ersetzt die zweite Fassung (ISO/IEC 15408-1:2005), die technisch überarbeitet wurde.

ISO/IEC 15408 besteht unter dem allgemeinen Titel *Information technology — Security techniques — Evaluation criteria for IT security* aus den folgenden Teilen:

- *Part 1: Introduction and general model*
- *Part 2: Security functional components*
- *Part 3: Security assurance components*

Diese korrigierte Version der ISO/IEC 15408-1:2009 enthält die folgenden, allgemeinen redaktionellen Korrekturen:

- Terminologie: Korrekturen für die Begriffe „Sicherheitsproblem“ und „Sicherheitsdomäne“;
- 8.3: Erklärung der strikten Konformität, Entfernung von vorherigem Bild 4.

Einleitung

Die ISO/IEC 15408 ermöglicht die Vergleichbarkeit von Ergebnissen unabhängiger Sicherheitsbewertungen. Die ISO/IEC 15408 erreicht dies durch eine einheitliche Reihe von Anforderungen an die Sicherheitsfunktionalität von IT-Produkten und an Maßnahmen zur Zusicherung der Vertrauenswürdigkeit, die auf diese IT-Produkte während einer Sicherheitsevaluierung angewendet werden. Diese IT-Produkte dürfen in Hardware, Firmware oder Software implementiert werden.

Durch den Evaluierungsprozess wird ein Vertrauensniveau hergestellt, dass die Sicherheitsfunktionalität dieser IT-Produkte und die auf diese IT-Produkte angewendeten Maßnahmen zur Zusicherung der Vertrauenswürdigkeit diese Anforderungen erfüllen. Die Evaluierungsergebnisse können die Verbraucher bei der Bestimmung unterstützen, ob diese IT-Produkte ihre Sicherheitsbedürfnisse erfüllen.

Die ISO/IEC 15408 ist hilfreich als Leitfaden für Entwicklung, Evaluierung und/oder Beschaffung von IT-Produkten mit Sicherheitsfunktionalität.

Die ISO/IEC 15408 ist absichtlich flexibel gestaltet, um einen großen Bereich an Evaluierungsmethoden für einen großen Bereich an Sicherheitseigenschaften einer Vielzahl von IT-Produkten abzudecken. Anwender dieser Norm werden daher darauf hingewiesen, sorgfältig vorzugehen, damit diese Flexibilität nicht zweckentfremdet wird. Wird die ISO/IEC 15408 beispielsweise in Verbindung mit ungeeigneten Evaluierungsmethoden, irrelevanten Sicherheitseigenschaften oder unangemessenen IT-Produkten verwendet, kann dies zu bedeutungslosen Evaluierungsergebnissen führen.

Somit hat die Evaluierung eines IT-Produkts nur eine Bedeutung im Zusammenhang mit den beurteilten Sicherheitseigenschaften und den angewendeten Evaluierungsmethoden. Evaluierungsinstanzen wird empfohlen, Produkte, Eigenschaften und Methoden zur Bestimmung, ob eine Evaluierung bedeutungsvolle Ergebnisse liefern wird, sorgfältig zu prüfen. Zusätzlich wird Käufern evaluierter Produkte empfohlen, sorgfältig zu prüfen, ob das evaluierte Produkt in diesem Zusammenhang und für die bestimmte Situation und ihre Bedürfnisse sinnvoll und anwendbar ist.

Die ISO/IEC 15408 behandelt den Schutz von Vermögenswerten vor unautorisierter Offenlegung, Änderung oder Nutzungsausfall. Die Schutzkategorien für diese drei Ausfalltypen der Sicherheit werden allgemein Vertraulichkeit, Integrität und Verfügbarkeit genannt. Die ISO/IEC 15408 kann auch anwendbar sein auf Bereiche der IT-Sicherheit, die über diese drei Kategorien hinausgehen. Die ISO/IEC 15408 ist anwendbar auf von Menschen ausgelöste Risiken (böswillig oder anders geartet) und auf nicht von Menschen ausgelöste Risiken. Die ISO/IEC 15408 darf neben der IT-Sicherheit auch auf andere Bereiche der IT angewendet werden, aber die Norm erhebt für jene anderen Bereiche keinen Anspruch auf Anwendbarkeit.

Bestimmte Themen liegen außerhalb des Anwendungsbereichs der ISO/IEC 15408, weil sie besondere Techniken umfassen oder nur am Rande Teil der IT-Sicherheit sind. Einige dieser Themen sind unten aufgeführt.

- a) ISO/IEC 15408 umfasst keine Sicherheitsevaluierungskriterien zu administrativen Sicherheitsmaßnahmen, die sich nicht direkt auf die IT-Sicherheitsfunktionalität beziehen. Allerdings ist es eine anerkannte Tatsache, dass eine beträchtliche Erhöhung der Sicherheit oftmals durch administrative Maßnahmen im organisatorischen, personellen, physischen oder verfahrenstechnischem Bereich erreicht werden kann oder dadurch unterstützt wird.
- b) Auf die Evaluierung einiger technisch-physikalischer Aspekte der IT-Sicherheit wie elektromagnetische Emanationssteuerung wird nicht im Speziellen eingegangen, obwohl eine Vielzahl der behandelten Konzepte auf dieses Gebiet anwendbar sind.

- c) Die ISO/IEC 15408 behandelt nicht die Evaluierungsmethodologie, mit der die Kriterien angewendet werden sollten. Diese Methodologie ist in der ISO/IEC 18045 enthalten.
- d) Die ISO/IEC 15408 behandelt nicht das administrative und rechtliche Rahmenwerk, mit dem die Kriterien von Evaluierungsinstanzen angewendet werden dürfen. Es wird jedoch erwartet, dass die ISO/IEC 15408 für Evaluierungszwecke im Zusammenhang mit einem solchen Rahmenwerk verwendet wird.
- e) Die Verfahren zur Verwendung von Evaluierungsergebnissen in Akkreditierungen liegen außerhalb des Anwendungsbereichs der ISO/IEC 15408. Akkreditierung ist der administrative Prozess, bei dem die Berechtigung für den Betrieb eines IT-Produkts (oder einer Sammlung dergleichen) in seiner vollständigen Betriebsumgebung gewährt wird, einschließlich aller seiner Nicht-IT-Teile. Die Ergebnisse des Evaluierungsprozesses fließen in den Akkreditierungsprozess ein. Da allerdings andere Techniken für die Bewertung von Eigenschaften ohne Bezug zur IT und deren Beziehung zu Teilen der IT-Sicherheit besser geeignet sind, sollten Akkreditierer gesonderte Vorkehrungen für diese Aspekte treffen.
- f) Die Kriterien für die Bewertung der charakteristischen Qualitäten von kryptographischen Algorithmen werden nicht in der ISO/IEC 15408 behandelt. Sollte eine unabhängige Bewertung der mathematischen Eigenschaften der Kryptographie erforderlich sein, so muss der unter der ISO/IEC 15408 angewendete Evaluierungsplan solch eine Bewertung vorsehen.

Die im Dokument durchgängig verwendete ISO-Terminologie wie „kann“, „informativ“, „darf“, „normativ“, „muss“ und „sollte“ sind in den ISO-/IEC-Richtlinien, Teil 2 festgelegt. Es ist zu beachten, dass der Begriff „sollte“ bei der Anwendung dieser Norm noch eine zusätzliche Bedeutung hat. Siehe Anmerkung unten. Die folgende Definition gilt für die Verwendung von „sollte“ in der ISO/IEC 15408:

sollte

In normativen Texten zeigt „sollte“ an, „dass unter verschiedenen Möglichkeiten eine Möglichkeit als besonders zutreffend empfohlen wird, ohne andere zu erwähnen oder auszuschließen, oder dass eine bestimmte Vorgehensweise bevorzugt wird, aber nicht notwendigerweise erforderlich ist.“ (ISO/IEC-Richtlinien, Teil 2).

ANMERKUNG ISO/IEC 15408 interpretiert „nicht notwendigerweise erforderlich“ so, dass die Wahl zugunsten einer anderen Möglichkeit eine Begründung zur Nichtverwendung der bevorzugten Option erfordert.

1 Anwendungsbereich

Dieser Teil der ISO/IEC 15408 legt die allgemeinen Konzepte und Prinzipien der IT-Sicherheitsbewertung fest und bestimmt das allgemeine Bewertungsmodell, das in vielen Teilen der Norm verwendet wird, und das in seiner Gesamtheit als Grundlage für die Bewertung der Sicherheitseigenschaften von IT-Produkten vorgesehen ist.

Teil 1 bietet einen Überblick über alle Teile der Norm ISO/IEC 15408. Dieser Teil beschreibt die verschiedenen Teile der Norm, definiert die Begriffe und Abkürzungen zur Verwendung in allen Teilen der Norm, legt das Kernkonzept des Bewertungsgegenstands (TOE; en: target of evaluation) und den Bewertungszusammenhang fest und beschreibt die Zielgruppe, an die sich die Bewertungskriterien richten. Zu den für die Bewertung von IT-Produkten erforderlichen, grundlegenden Sicherheitskonzepten wird eine Einführung gegeben.

Diese Einführung definiert die verschiedenen Operationen, mit denen die Funktionskomponenten und Vertrauenswürdigkeitskomponenten in ISO/IEC 15408-2 und ISO/IEC 15408-3 für die Verwendung der zulässigen Operationen angepasst werden dürfen.

Die grundlegenden Konzepte von Schutzprofilen (PP; en: protection profiles), Paketen, Sicherheitsanforderungen und das Thema Konformität werden spezifiziert und die Konsequenzen von Bewertung und Bewertungsergebnissen beschrieben. Dieser Teil der ISO/IEC 15408 enthält Leitlinien für die Spezifizierung von Sicherheitsvorgaben (ST; en: security targets) und beschreibt die Organisation von Bestandteilen im gesamten Modell. Die ISO/IEC 18045 enthält allgemeine Informationen über die Bewertungsmethodologie und bestimmt den Anwendungsbereich von Bewertungsplänen.

2 Normative Verweisungen

Die folgenden zitierten Dokumente sind für die Anwendung von ISO/IEC 15408 Teil 1 erforderlich. 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 15408-2, *Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional components*

ISO/IEC 15408-3, *Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance components*

ISO/IEC 18045, *Information technology — Security techniques — Methodology for IT security evaluation*

3 Begriffe

Für die Anwendung dieses Dokuments gelten die folgenden Begriffe.

ANMERKUNG Dieser Abschnitt enthält nur diejenigen Begriffe, die innerhalb von ISO/IEC 15408 in spezieller Weise verwendet werden. Manche Kombinationen von in ISO/IEC 15408 verwendeten allgemeinen Begriffen sind daher nicht in diesem Abschnitt enthalten, werden aber der Klarheit wegen in dem Zusammenhang erläutert, in dem sie verwendet werden.

3.1 In ISO/IEC 15408 verwendete Begriffe

3.1.1

nachteilige Aktionen

Aktionen, die von einem Bedrohungsagenten gegen ein Schutzobjekt durchgeführt werden

3.1.2

Schutzobjekte

Entitäten, von denen anzunehmen ist, dass sie für den Eigentümer des TOEs einen Wert darstellen

3.1.3

Zuweisung

Spezifikation eines bezeichneten Parameters in einer Komponente (von ISO/IEC 15408) oder einer Anforderung

3.1.4

Sicherheit

Vertrauensgrundlage, dass ein TOE die SFRs einhält

3.1.5

Angriffspotential

Maß für den erforderlichen Aufwand bei einem Angriff auf ein TOE, ausgedrückt in Form von Fachkenntnis, Ressourcen und Motivation des Angreifers

3.1.6

Erweiterung

Hinzufügen von einer oder mehreren Anforderung(en) zu einem Paket

3.1.7

Authentisierungsdaten

Informationen, die zur Überprüfung der angegebenen Identität eines Benutzers verwendet werden

3.1.8

autorisierter Benutzer

TOE-Benutzer, der in Übereinstimmung mit den SFRs eine Funktion durchführen darf

3.1.9

Klasse

eine Reihe von ISO/IEC 15408-Familien mit einem gemeinsamen Fokus

3.1.10

kohärent

logisch geordnet und mit einer erkennbaren Bedeutung

ANMERKUNG Im Zusammenhang mit Dokumentation bezieht sich dies sowohl auf den eigentlichen Text als auch auf die Struktur des Dokuments hinsichtlich der Verständlichkeit für die Zielgruppe.

3.1.11

vollständig

Eigenschaft, die angibt, dass alle erforderlichen Teile einer Entität bereitgestellt wurden

ANMERKUNG In Bezug auf Dokumentation bedeutet dies, dass alle relevanten Informationen in der Dokumentation in einer solchen Detailliertheit beschrieben sind, dass auf der entsprechenden Abstraktionsebene keine weitere Erklärung erforderlich ist.

3.1.12

Komponente

kleinster selektierbarer Elementesatz, auf dem Anforderungen basieren können

3.1.13

zusammengesetztes Sicherheitspaket

CAP

(en: Composed Assurance Package)

Sicherheitspaket, bestehend aus Anforderungen, die auf ISO/IEC 15408-3 beruhen (vorwiegend auf der ACO-Klasse) und die einen Punkt der in ISO/IEC 15408 definierten zusammengesetzten Sicherheitsskala repräsentieren

3.1.14

bestätigen

erklären, dass etwas detailliert und mit einer unabhängig bestimmten Angemessenheit geprüft wurde

ANMERKUNG Die erforderliche Stringenz hängt von der Art der betrachteten Einheit ab. Dieser Begriff wird nur für Evaluatorenaktionen verwendet.

3.1.15

Konnektivität

Eigenschaft des TOEs, die eine Interaktion mit IT-Entitäten außerhalb des TOEs ermöglicht

ANMERKUNG Dies schließt den Datenaustausch über verdrahtete oder drahtlose Verbindungen, über beliebige Entfernungen und in allen Umgebungen und Konfigurationen ein.

3.1.16

widerspruchsfrei

Beziehung zwischen zwei oder mehreren Entitäten, bei der keine offensichtlichen Widersprüche zwischen diesen Entitäten auftreten

3.1.17

abwehren, Verb

einem Angriff entgegenwirken, wobei die Auswirkung einer bestimmten Bedrohung abgemildert, aber nicht notwendigerweise ausgeremert wird

3.1.18

nachweisliche Konformität

Beziehung zwischen einer ST und einem PP, wobei die ST eine Lösung bereitstellt, welche das generische Sicherheitsproblem im PP löst

ANMERKUNG Das PP und die ST können völlig unterschiedliche Aussagen enthalten, die verschiedene Entitäten behandeln, verschiedene Konzepte verwenden usw. Die nachweisliche Konformität eignet sich auch für TOE-Typen, für die bereits mehrere ähnliche PPs existieren, so dass der ST-Autor auch die Konformität mit diesen PPs beanspruchen kann, um so Arbeit zu ersparen.

3.1.19

nachweisen

eine Schlussfolgerung liefern, die durch eine weniger strenge Analyse als einen „Beweis“ erlangt wurde

3.1.20

Abhängigkeit

Verhältnis zwischen Komponenten, bei dem gilt, dass wenn eine auf der abhängigen Komponente basierende Anforderung in einem PP, einer ST oder einem Paket enthalten ist, normalerweise auch eine Anforderung im PP, in der ST oder im Paket enthalten sein muss, die auf der Komponente basiert, von der die Abhängigkeit besteht

3.1.21

beschreiben

spezifische Einzelheiten zu einer Entität bereitstellen

3.1.22

bestimmen

eine bestimmte Schlussfolgerung auf Basis einer unabhängigen Analyse bestätigen mit dem Ziel, eine bestimmte Schlussfolgerung zu erreichen

ANMERKUNG Die Verwendung dieses Begriffs setzt eine wirklich unabhängige Analyse voraus, in der Regel ohne dass eine vorhergehende Analyse durchgeführt wurde. Vergleiche die Begriffe „bestätigen“ oder „verifizieren“, welche voraussetzen, dass bereits eine Analyse durchgeführt wurde, welche überprüft werden muss.

3.1.23

Entwicklungsumgebung

Umgebung, in der der TOE entwickelt wird

3.1.24

Element

nicht unterteilbare Beschreibung einer Sicherheitsanforderung

3.1.25

sicherstellen

eine starke kausale Abhängigkeit zwischen einer Aktion und deren Auswirkungen garantieren

ANMERKUNG Wenn diesem Begriff das Wort „helfen“ vorangestellt ist, weist dies darauf hin, dass die Auswirkung aufgrund nur dieser Aktion nicht sicher garantiert ist.

3.1.26

Evaluierung

Bewertung eines PP, einer ST oder eines TOEs auf Grundlage definierter Kriterien

3.1.27

Vertrauenswürdigkeitsstufe

EAL-Stufe

(en: Evaluation Assurance Level)

Reihe von aus ISO/IEC 15408-3 entnommenen Vertrauenswürdigkeitsanforderungen, die einem Punkt der in ISO/IEC 15408 definierten Vertrauenswürdigkeitsskala entsprechen, welche ein Sicherheitspaket bilden

3.1.28

Evaluierungsinstanz

Institution, die für von Institutionen innerhalb einer bestimmten Gemeinschaft durchgeführte Evaluierungen die Anforderungen festlegt und die Qualität überwacht und die mittels eines Evaluierungsprogramms ISO/IEC 15408 für die jeweilige Gemeinschaft implementiert

3.1.29

Evaluierungsprogramm

administratives und regulatorisches Rahmenwerk, auf dessen Basis ISO/IEC 15408 innerhalb einer bestimmten Gemeinschaft durch eine Evaluierungsinstanz umgesetzt wird

3.1.30

erschöpfend

Merkmal eines methodischen Konzepts zur Durchführung einer Analyse oder Aktivität in Übereinstimmung mit einem eindeutigen Plan

ANMERKUNG Dieser Begriff wird in ISO/IEC 15408 bezüglich der Durchführung einer Analyse oder einer anderen Aktivität verwendet. Er ist mit „systematisch“ verwandt, ist aber erheblich stärker, da er nicht nur angibt, dass zur Durchführung der Analyse oder Aktivität ein methodischer Ansatz nach einem eindeutigen Plan befolgt wurde, sondern auch, dass der befolgte Plan ausreicht, um sicherzustellen, dass alle möglichen Verfahrensweisen durchgeführt wurden.

3.1.31 erklären

ein Argument für die Begründung einer gewählten Vorgehensweise liefern

ANMERKUNG Dieser Begriff unterscheidet sich von den Begriffen „beschreiben“ und „demonstrieren“. Er soll die Frage nach dem „Warum“ beantworten, ohne Argumente dafür zu liefern, dass die gewählte Vorgehensweise notwendigerweise optimal war.

3.1.32 Erweiterung

Hinzufügen von funktionellen Anforderungen, die nicht in ISO/IEC 15408-2 enthalten sind, zu einer ST oder PP und/oder Hinzufügen von Sicherheitsanforderungen, die nicht in ISO/IEC 15408-3 enthalten sind

3.1.33 externe Entität

menschliche oder IT-Entität, die möglicherweise von außerhalb der TOE-Grenze mit dem TOE interagiert

ANMERKUNG Eine externe Entität kann auch als Benutzer bezeichnet werden.

3.1.34 Familie

Satz von Komponenten, die eine ähnliche Zielsetzung haben, sich aber in Schwerpunkt oder Stringenz unterscheiden

3.1.35 formal

ausgedrückt in einer Sprache mit begrenzter Syntax und definierter Semantik, basierend auf anerkannten mathematischen Konzepten

3.1.36 Leitliniendokumentation

Dokumentation, die die Auslieferung, die Bereitstellung, den Betrieb, das Management und/oder die Verwendung des TOEs beschreibt

3.1.37 Identität

Repräsentation, mit der Entitäten im Zusammenhang mit dem TOE eindeutig identifiziert werden (z. B. Benutzer, Prozesse oder Festplatten)

ANMERKUNG Ein Beispiel für eine solche Repräsentation ist eine Zeichenkette. Bei einem menschlichen Benutzer kann die Repräsentation der vollständige oder abgekürzte Name oder ein (nach wie vor eindeutiges) Pseudonym sein.

3.1.38 informal

in der natürlichen Sprache ausgedrückt

3.1.39 Inter-TSF-Übertragung

Datenkommunikation zwischen dem TOE und den Sicherheitsfunktionen anderer vertrauenswürdiger IT-Produkte

3.1.40 interner Kommunikationskanal

Kommunikationskanal zwischen getrennten Teilen des TOEs

3.1.41

interne TOE-Übertragung

Datenkommunikation zwischen getrennten Teilen des TOEs

3.1.42

in sich widerspruchsfrei

es bestehen keine offensichtlichen Widersprüche zwischen irgendwelchen Aspekten einer Entität

ANMERKUNG In Bezug auf Dokumentation bedeutet dies, dass keine Aussagen in der Dokumentation enthalten sein können, die als widersprüchlich zueinander interpretiert werden können.

3.1.43

Iteration

Verwendung der gleichen Komponente, um zwei oder mehr unterschiedliche Anforderungen auszudrücken

3.1.44

Begründung

Analyse, die zu einer Schlussfolgerung führt

ANMERKUNG „Begründung“ ist stringenter als ein Nachweis. Dieser Begriff erfordert erhebliche Stringenz, indem jeder Schritt eines logischen Arguments sehr sorgfältig und gründlich erläutert wird.

3.1.45

Objekt

passive Entität im TOE, die Informationen enthält oder empfängt und an der Subjekte Operationen durchführen

3.1.46

Operation

<an einer Komponente von ISO/IEC 15408> Modifikation oder Wiederholung einer Komponente

ANMERKUNG Zulässige Operationen an Komponenten sind Zuweisung, Iteration, Präzisierung und Auswahl.

3.1.47

Operation

<an einem Objekt> spezifische Aktion, die durch ein Subjekt an einem Objekt durchgeführt wird

3.1.48

Betriebsumgebung

Umgebung, in der der TOE betrieben wird

3.1.49

organisatorische Sicherheitspolitik

OSP

(en: Organisational Security Policy)

Satz von Sicherheitsregeln, -verfahren oder -leitlinien für eine Organisation

ANMERKUNG Eine Politik kann sich auf eine spezifische Betriebsumgebung beziehen.

3.1.50

Paket

benannter Satz von Anforderungen bezüglich der Sicherheitsfunktionalität oder Vertrauenswürdigkeit

ANMERKUNG Ein Beispiel für ein Paket ist „EAL 3“.

3.1.51

Schutzprofilevaluierung

Bewertung eines PP auf Grundlage definierter Kriterien

3.1.52

Schutzprofil

PP

(en: Protection Profile)

implementierungsunabhängige Beschreibung der Sicherheitsanforderungen für einen TOE-Typ

3.1.53

beweisen

Übereinstimmung im mathematischen Sinn durch formale Analyse aufzeigen

ANMERKUNG Der Begriff ist in jeder Beziehung vollständig stringent. Im Allgemeinen wird „beweisen“ verwendet, wenn die Übereinstimmung zwischen zwei TSF-Darstellungen auf einem hohen Stringenzniveau dargestellt werden soll.

3.1.54

Präzisierung

Hinzufügen von Details zu einer Komponente

3.1.55

Rolle

vordefinierter Regelsatz, der die zulässigen Interaktionen zwischen einem Benutzer und dem TOE festlegt

3.1.56

Geheimnis

Informationen, die nur autorisierten Benutzern und/oder der TSF bekannt sein dürfen, um ein spezifisches SFP durchzusetzen

3.1.57

sicherer Zustand

Zustand, in dem die TSF-Daten konsistent sind und die TSF die ordnungsgemäße Durchsetzung der SFRs fortlaufend wahrnimmt

3.1.58

Sicherheitsattribut

Eigenschaft von Subjekten, Benutzern (einschließlich externen IT-Produkten), Objekten, Informationen, Sitzungen und/oder Ressourcen, die verwendet wird, um die SFRs zu definieren, und deren Werte zur Durchsetzung der SFRs verwendet werden

3.1.59

Sicherheitsfunktionspolitik

SFP

(en: Security Function Policy)

Regelsatz, der ein bestimmtes Sicherheitsverhalten beschreibt, das von der TSF durchgesetzt wird und sich als ein Satz von SFRs beschreiben lässt

3.1.60

Sicherheitszielsetzung

(en: Security Objective)

Absichtserklärung, identifizierte Bedrohungen abzuwehren und/oder identifizierte organisatorische Sicherheitspolitiken und/oder -annahmen zu erfüllen

3.1.61

Sicherheitsproblem

Aussage, die formal die Natur und den Geltungsbereich der Sicherheit definiert, welche den TOE adressieren soll

ANMERKUNG Diese Aussage besteht aus folgenden Teilen:

- den Bedrohungen, die durch den TOE und seine Betriebsumgebung abgewehrt werden sollen,
- den OSPs, die durch den TOE und seine Betriebsumgebung durchgesetzt werden, und
- den Annahmen, die für die Betriebsumgebung des TOEs bestehen.

3.1.62

Sicherheitsanforderung

in einer standardisierten Sprache ausgedrückte Anforderung, die zur Erreichung der Sicherheitsziele für ein TOE beitragen soll

3.1.63

Sicherheitsvorgabe

ST

(en: Security Target)

implementierungsabhängige Beschreibung der Sicherheitsanforderungen für einen spezifischen, identifizierten TOE

3.1.64

Auswahl

Spezifikation eines oder mehrerer Element(e) aus einer Liste innerhalb einer Komponente

3.1.65

semiformal

ausgedrückt in einer Sprache mit begrenzter Syntax und definierter Semantik

3.1.66

spezifizieren

auf stringente und präzise Weise spezifische Einzelheiten zu einer Entität bereitstellen

3.1.67

strikte Konformität

hierarchische Beziehung zwischen einer ST und einem PP, wobei alle Anforderungen im PP auch in der ST vorhanden sind

ANMERKUNG Diese Beziehung kann grob definiert werden als: „die ST muss alle Aussagen enthalten, die im PP vorhanden sind, darf aber weitere enthalten“. Es wird erwartet, dass strikte Konformität für stringente Anforderungen eingesetzt wird, die in konsistenter Weise erfüllt werden müssen.

3.1.68

ST-Evaluierung

Bewertung einer ST auf Grundlage definierter Kriterien

3.1.69

Subjekt

aktive Entität im TOE, die Operationen an Objekten durchführt

3.1.70

Evaluierungsgegenstand

TOE

(en: Target of Evaluation)

Satz von Software, Firmware und/oder Hardware, möglicherweise mit beigefügten Leitlinien

3.1.71

Bedrohungsagent

Entität, die auf Schutzobjekte nachteilig einwirken kann

3.1.72

TOE-Evaluierung

Bewertung eines TOEs auf Grundlage definierter Kriterien

3.1.73

TOE-Ressource

alles, was innerhalb des TOEs nutzbar oder verwertbar ist

3.1.74

TOE-Sicherheitsfunktionalität

(en: TOE Security Functionality)

kombinierte Funktionalität der gesamten Hardware, Software und Firmware eines TOEs, welche die korrekte Durchsetzung der SFRs sicherstellen muss

3.1.75

verfolgen, Verb

Durchführen einer informalen Korrespondenzanalyse zwischen zwei Entitäten mit nur minimaler Stringenz

3.1.76

Übertragungen außerhalb des TOEs

TSF-vermittelte Kommunikation von Daten an Entitäten, die nicht der Kontrolle der TSF unterliegen

3.1.77

Übersetzung

beschreibt den Prozess der Beschreibung von Sicherheitsanforderungen in einer standardisierten Sprache

ANMERKUNG Die Verwendung des Begriffs „Übersetzung“ ist in diesem Zusammenhang nicht wörtlich zu nehmen; es wird nicht impliziert, dass jedes in standardisierter Sprache ausgedrückte SFR wieder in die Sicherheitszielsetzungen zurückübersetzt werden kann.

3.1.78

vertrauenswürdiger Kanal

ein Weg, über den ein TSF und ein anderes vertrauenswürdigen IT-Produkt mit dem notwendigen Vertrauensgrad kommunizieren können

3.1.79

vertrauenswürdigen IT-Produkt

IT-Produkt (nicht der TOE), dessen funktionelle Sicherheitsanforderungen administrativ mit dem TOE koordiniert sind und von dem angenommen wird, dass es die funktionellen Sicherheitsanforderungen korrekt implementiert

ANMERKUNG Ein Beispiel für ein vertrauenswürdigen IT-Produkt wäre ein Produkt, das getrennt evaluiert wurde.

3.1.80

vertrauenswürdigen Pfad

Weg, über den ein Anwender und ein TSF mit dem notwendigen Vertrauensgrad kommunizieren können

3.1.81

TSF-Daten

Daten für den Betrieb des TOEs, welche für die Durchsetzung des SFR benötigt werden

3.1.82

TSF-Schnittstelle

(en: TSF Interface)

Weg, über den externe Entitäten (oder Subjekte im TOE, die nicht Teil des TSF sind) Daten an das TSF übermitteln, Daten vom TSF empfangen und Dienste des TSF aufrufen

3.1.83

Benutzerdaten

Daten für den Benutzer, die nicht den Betrieb des TSF beeinflussen

3.1.84

verifizieren

streng, detailliert und mit einer unabhängig bestimmten Angemessenheit prüfen

ANMERKUNG Siehe auch „bestätigen“. Dieser Begriff hat eine strengere Bedeutung. Der Begriff „verifizieren“ wird im Zusammenhang mit Evaluatorenaktionen verwendet, wenn eine unabhängige Anstrengung durch den Evaluator erforderlich ist.

3.2 Begriffe in Zusammenhang mit der Klasse ADV

ANMERKUNG Die folgenden Begriffe werden in den Anforderungen an die interne Software-Struktur verwendet. Einige sind entnommen aus IEEE Standard 610.12-1990, *Standard glossary of software engineering terminology*, Institute of Electrical and Electronics Engineers.

3.2.1

Administrator

Entität, die bezüglich aller durch das TSF implementierten Politiken einen Vertrauensgrad besitzt

ANMERKUNG Nicht alle PPs und STs nehmen für Administratoren den gleichen Vertrauensgrad an. Üblicherweise wird angenommen, dass Administratoren jederzeit die in der ST des TOEs definierten Politiken einhalten. Manche dieser Politiken können mit der Funktionalität des TOEs in Zusammenhang stehen, andere mit der Betriebsumgebung.

3.2.2

Aufrufbaum

identifiziert die Module in einem System in Form eines Diagramms, das aufzeigt, welche Module sich gegenseitig aufrufen

ANMERKUNG Basierend auf IEEE Standard 610.12-1990.

3.2.3

Kohäsion

Modulstärke

Art und Grad, wie die von einem Software-Modul durchgeführten Aufgaben miteinander in Zusammenhang stehen

[IEEE Standard 610.12-1990]

ANMERKUNG Zu den Kohäsionsarten gehören die zufällige, die kommunikative, die funktionelle, die logische, die sequentielle und die zeitliche Kohäsion. Diese Kohäsionsarten werden beim entsprechenden Begriffseintrag beschrieben.

3.2.4

zufällige Kohäsion

Modul, das unzusammenhängende oder nur bedingt zusammenhängende Aktivitäten ausführt

[IEEE Standard 610.12-1990]

ANMERKUNG Siehe auch Kohäsion (3.2.3).

3.2.5

kommunikative Kohäsion

Modul, das Funktionen enthält, die Ausgaben für andere Funktionen innerhalb des Moduls produzieren oder Ausgaben anderer Funktionen innerhalb des Moduls nutzen

[IEEE Standard 610.12-1990]

ANMERKUNG 1 Siehe auch Kohäsion (3.2.3).

ANMERKUNG 2 Ein Beispiel für ein kommunikativ kohäsives Modul ist ein Zugriffsüberprüfungsmodul, das obligatorische, diskrete und Funktionsprüfungen enthält.

3.2.6

Komplexität

Maßwert dafür, wie schwierig Software zu verstehen und daher zu analysieren, testen und warten ist

[IEEE Standard 610.12-1990]

ANMERKUNG Die Reduzierung der Komplexität ist das oberste Ziel beim Einsatz von modularer Aufteilung, Schichtung und Minimierung. Die Kontrolle von Kopplung und Kohäsion trägt erheblich zur Erreichung dieses Ziels bei.

Im Bereich des Software-Engineering wurde erheblicher Aufwand in den Versuch investiert, Metriken zur Messung der Komplexität von Quellcode zu entwickeln. Die meisten dieser Metriken nutzen einfach zu berechnende Eigenschaften des Quellcodes, wie beispielsweise die Anzahl von Operatoren und Operanden, die Komplexität des Kontrollflussgraphen (zyklomatische Komplexität), die Anzahl der Quellcode-Zeilen, das Verhältnis zwischen Kommentaren und ausführbarem Code und ähnliche Maßwerte. Kodierungsstandards haben sich als wertvolles Instrument zur Erzeugung von Code erwiesen, der einfacher zu verstehen ist.

Die Familie der TSF-Interna (ADV_INT) erfordert eine Komplexitätsanalyse aller Komponenten. Es wird erwartet, dass der Entwickler Nachweise für die Behauptung liefert, dass die Komplexität ausreichend reduziert wurde. Diese Nachweise können beispielsweise die Programmierstandards des Entwicklers enthalten sowie eine Angabe, dass alle Module den Standards entsprechen (oder dass es einige Ausnahmen gibt, die durch Software-Engineering-Argumente begründet sind). Sie könnten die Ergebnisse von Werkzeugen enthalten, die zur Messung mancher Eigenschaften des Quellcodes eingesetzt wurden, oder andere Nachweise, die der Entwickler für angemessen hält.

3.2.7

Kopplung

Art und Grad der gegenseitigen Abhängigkeit von Software-Modulen

[IEEE Standard 610.12-1990]

ANMERKUNG Zu den Kopplungsarten gehören die Aufrufkopplung, die Bereichskopplung und die Inhaltskopplung. Diese sind nachstehend beschrieben.

3.2.8

Aufrufkopplung

Beziehung zwischen zwei Modulen, die strikt nur über ihre dokumentierten Funktionsaufrufe kommunizieren

ANMERKUNG Beispiele für die Aufrufkopplung sind die Daten-, Datenstruktur- und Kontrollkopplung.

3.2.9

Aufrufkopplung

<Datenkopplung> Beziehung zwischen zwei Modulen, die strikt nur durch die Verwendung von Aufrufparametern kommunizieren, die einzelnen Datenelementen entsprechen

ANMERKUNG Siehe auch Aufrufkopplung (3.2.8).

3.2.10

Aufrufkopplung

<Datenstrukturkopplung> Beziehung zwischen zwei Modulen, die durch die Verwendung von Aufrufparametern kommunizieren, die mehrere Felder umfassen oder die sinnvolle interne Strukturen haben

ANMERKUNG Siehe auch Aufrufkopplung (3.2.8).

3.2.11

Aufrufkopplung

<Kontrollkopplung> Beziehung zwischen zwei Modulen, wobei ein Modul Informationen weitergibt, welche die interne Logik des anderen Moduls beeinflussen sollen

ANMERKUNG Siehe auch Aufrufkopplung (3.2.8).

3.2.12

Bereichskopplung

Beziehung zwischen zwei Modulen, die sich einen gemeinsamen Datenbereich oder eine andere gemeinsame Systemressource teilen

ANMERKUNG Globale Variablen zeigen an, dass die Module, die diese globalen Variablen verwenden, über eine Bereichskopplung verfügen. Die Bereichskopplung mittels globaler Variablen ist allgemein zulässig, aber nur in einem begrenzten Ausmaß.

Beispielsweise sind Variablen, die in einem globalen Bereich platziert sind, aber nur von einem einzigen Modul verwendet werden, unpassend platziert und sollten entfernt werden. Weitere Faktoren, die bei der Bewertung der Eignung globaler Variablen berücksichtigt werden müssen, sind:

Die Anzahl der Module, die eine globale Variable modifizieren: Im Allgemeinen sollte nur ein einziges Modul die Kontrolle des Inhalts einer globalen Variablen wahrnehmen, aber es kann Situationen geben, in denen ein zweites Modul diese Aufgabe ebenfalls wahrnimmt; in solchen Fällen muss eine ausreichende Begründung geliefert werden. Es ist nicht annehmbar, dass diese Aufgabe von mehr als zwei Modulen wahrgenommen wird. (Bei der Durchführung dieser Bewertung sollte sorgfältig bestimmt werden, welches Modul tatsächlich für den Inhalt der Variablen verantwortlich ist. Wenn die Variable beispielsweise nur von einer Routine modifiziert wird, aber diese Routine einfach nur die vom aufrufenden Modul angeforderte Modifikation durchführt, dann ist das aufrufende Modul verantwortlich, und es könnten mehrere solcher Module vorhanden sein). Wenn zwei Module für den Inhalt einer globalen Variablen zuständig sind, sollte des Weiteren als Teil der Komplexitätsbewertung klar definiert sein, wie die Modifikationen zwischen den Modulen koordiniert werden.

Die Anzahl der Module, die eine globale Variable referenzieren: Auch wenn es keinen allgemeinen Grenzwert für die Anzahl der Module gibt, die eine globale Variable referenzieren, sollte in Fällen, in denen viele Module eine solche Referenzierung durchführen, die Gültigkeit und Notwendigkeit untersucht werden.

3.2.13

Inhaltskopplung

Beziehung zwischen zwei Modulen, wobei ein Modul die Interna des anderen Moduls direkt referenziert

ANMERKUNG Beispiele sind die Modifizierung des Codes oder die Referenzierung von internen Labels des anderen Moduls. Daraus ergibt sich, dass ein Teil oder der gesamte Inhalt eines Moduls effektiv im anderen Modul enthalten ist. Die Inhaltskopplung kann als die Verwendung nicht offengelegter Modulschnittstellen betrachtet werden, im Gegensatz zur Aufrufkopplung, bei der nur offengelegte Modulschnittstellen verwendet werden.

3.2.14

Domänentrennung

Eigenschaft von Sicherheitsarchitekturen, wobei das TSF getrennte Sicherheitsdomänen für jeden Benutzer und für das TSF definiert und sicherstellt, dass kein Benutzerprozess den Inhalt der Sicherheitsdomäne eines anderen Benutzers oder des TSF beeinflussen kann

3.2.15

funktionelle Kohäsion

funktionelle Eigenschaft eines Moduls, das nur Aktivitäten für eine einzige Aufgabe durchführt

[IEEE Standard 610.12-1990]

ANMERKUNG Ein funktionell kohäsives Modul wandelt eine einzige Eingabeart in eine einzige Ausgabeart um, wie beispielsweise ein Stack-Manager oder ein Warteschlangen-Manager. Siehe auch Kohäsion (3.2.3).

3.2.16

Interaktion

allgemeine, auf Kommunikation basierende Aktivität zwischen Entitäten

3.2.17

Schnittstelle

Mittel zur Interaktion mit einer Komponente oder einem Modul

3.2.18

Schichtung

Entwurfstechnik, bei der getrennte Modulgruppen (die Schichten) hierarchisch so organisiert sind, dass sie getrennte Zuständigkeiten besitzen, wobei eine Schicht nur die Dienste der in der Hierarchie darunterliegenden Schichten nutzt und die eigenen Dienste nur den darüberliegenden Schichten zur Verfügung stellt

ANMERKUNG Bei einer strengen Schichtung gilt zusätzlich, dass jede Schicht nur die Dienste der unmittelbar darunterliegenden Schicht nutzen kann und ihre Dienste nur für die unmittelbar darüberliegende Schicht zur Verfügung stellt.

3.2.19

logische Kohäsion

prozedurale Kohäsion

Merkmale eines Moduls, das ähnliche Aktivitäten an verschiedenen Datenstrukturen durchführt

ANMERKUNG Ein Modul weist eine logische Kohäsion auf, wenn seine Funktionen verwandte, aber unterschiedliche Operationen an verschiedenen Eingaben durchführen. Siehe auch „Kohäsion“.

3.2.20

modulare Aufteilung

Prozess der Aufteilung eines Systems in Komponenten, um den Entwurf, die Entwicklung und die Evaluierung zu vereinfachen

[IEEE Standard 610.12-1990]

3.2.21

Unumgänglichkeit

<des TSF> Eigenschaft einer Sicherheitsarchitektur, wobei alle Aktionen in Zusammenhang mit dem SFR vom TSF vermittelt werden

3.2.22

Sicherheitsdomänen

Umgebungen, die vom TSF für die Nutzung durch nicht vertrauenswürdige Entitäten derart bereitgestellt werden, dass diese Umgebungen isoliert und voreinander geschützt sind

3.2.23

sequentielle Kohäsion

Modul, das Funktionen enthält, deren Ausgaben als Eingaben für die jeweils folgenden Funktionen innerhalb des Moduls genutzt werden

[IEEE Standard 610.12-1990]

ANMERKUNG Ein Beispiel für ein sequentiell-kohäsives Modul ist ein Modul, das Funktionen zum Schreiben von Audit-Datensätzen und zur laufenden Zählung einer spezifischen Art von akkumulierten Audit-Verletzungen enthält.

3.2.24

Software-Engineering

Einsatz eines systematischen, disziplinierten und quantifizierbaren Verfahrens zur Entwicklung und Wartung von Software; kurz die Anwendung von Ingenieurwissenschaften auf Software

[IEEE Standard 610.12-1990]

ANMERKUNG Wie bei allen ingenieurwissenschaftlichen Praktiken ist bei der Anwendung der Engineering-Prinzipien ein gewisses Urteilsvermögen nötig. Entscheidungen werden durch eine Vielzahl von Faktoren beeinflusst, nicht nur durch die Anwendung von Maßnahmen zur modularen Aufteilung, Schichtung und Minimierung. So kann ein Entwickler beispielsweise ein System entwerfen, bei dem er zukünftige Applikationen berücksichtigt, die anfänglich nicht implementiert werden. Der Entwickler kann daher Logik einbinden, um diese zukünftigen Applikationen zu handhaben, ohne sie vollständig zu implementieren; des Weiteren kann der Entwickler Aufrufe von bisher nicht implementierten Modulen einschließen, so dass unvollständige Aufrufe (en: Call Stubs) entstehen. Bei der Beurteilung, ob solche Abweichungen von gut strukturierten Programmen durch den Entwickler gerechtfertigt sind, muss Urteilsvermögen und eine gute Software-Engineering-Disziplin zur Anwendung kommen.

3.2.25

zeitliche Kohäsion

Merkmal eines Moduls, das Funktionen enthält, die ungefähr gleichzeitig ausgeführt werden müssen

ANMERKUNG 1 Basierend auf [IEEE Standard 610.12-1990].

ANMERKUNG 2 Beispiele für zeitlich kohäsive Module sind Module für die Initialisierung, Wiederherstellung und Abschaltung.

3.2.26

TSF-Selbstschutz

Eigenschaft einer Sicherheitsarchitektur, wobei das TSF nicht von TSF-fremdem Code oder fremden Entitäten beschädigt werden kann

3.3 Begriffe in Zusammenhang mit der Klasse AGD

3.3.1

Installation

von einem menschlichen Benutzer durchgeführtes Verfahren zur Einbindung des TOEs in seine Betriebsumgebung und dessen Inbetriebnahme

ANMERKUNG Diese Operation wird normalerweise nur einmal nach Erhalt und Abnahme des TOEs durchgeführt. Es wird erwartet, dass der TOE soweit konfiguriert wird, dass die Konfiguration entsprechend der ST zulässig ist. Wenn ähnliche Prozesse durch den Entwickler durchgeführt werden müssen, dann werden sie im Rahmen der ALC: Produktlebenszyklusunterstützung als „Generierung“ bezeichnet. Falls der TOE eine Erstinbetriebnahme erfordert, die nicht regelmäßig wiederholt werden muss, dann würde dieser Prozess als Installation eingestuft.

3.3.2

Betrieb

Nutzungszeitraum des TOEs, einschließlich „übliche Nutzung“, Administration und Wartung des TOEs nach Auslieferung und Bereitstellung

3.3.3

Bereitstellung

Aktivität in der Lebenszyklusphase eines Produkts, die die Kundenabnahme des ausgelieferten TOE und dessen Installation umfasst, worunter Aktivitäten wie das Hochfahren, die Initialisierung, die Erstinbetriebnahme und die Vorbereitung des TOEs bis zu einem betriebsbereiten Zustand fallen können

3.4 Begriffe in Zusammenhang mit der Klasse ALC

3.4.1

Abnahmekriterien

während der Durchführung der Abnahmeverfahren anzuwendende Kriterien (z. B. erfolgreiche Dokumentationsprüfung oder, im Fall von Software, Firmware oder Hardware, erfolgreiche Funktionsprüfung)

3.4.2

Abnahmeverfahren

Verfahren, die durchgeführt werden, um neu erstellte oder geänderte Konfigurationselemente als Teil des TOEs zu akzeptieren oder in den nächsten Lebenszyklusschritt zu überführen

ANMERKUNG Diese Verfahren identifizieren die Rollen oder Einzelpersonen, die für die Abnahme verantwortlich sind, sowie die anzuwendenden Kriterien, die für die Entscheidung über die Abnahme herangezogen werden.

Es gibt mehrere Arten von Abnahmesituationen; manche können sich überschneiden:

- a) erstmalige Übernahme eines Elements in das Konfigurationsmanagementsystem, insbesondere Einbindung von Software-, Firmware- und Hardware-Komponenten anderer Hersteller in den TOE („Integration“);
- b) Überführung von Konfigurationselementen in die nächste Lebenszyklusphase in allen Entwurfsphasen des TOEs (z. B. Modul, Teilsystem, Qualitätskontrolle des fertiggestellten TOEs);
- c) im Anschluss an Transporte von Konfigurationselementen (z. B. Teilen des TOEs oder vorläufigen Produkten) zwischen verschiedenen Entwicklungsstandorten;
- d) im Anschluss an die Auslieferung des TOEs an den Verbraucher.

3.4.3

Konfigurationsmanagement

CM

(en: Configuration Management)

Fachgebiet, in dem technische und administrative Anleitung und Überwachung eingesetzt werden, um die funktionellen und physikalischen Merkmale eines Konfigurationselements zu identifizieren und zu dokumentieren, Änderungen dieser Merkmale zu kontrollieren, die Umsetzung von Änderungen sowie den Implementierungsstatus aufzuzeichnen und zu berichten und die Einhaltung der festgelegten Anforderungen zu überprüfen

ANMERKUNG Basierend auf IEEE Standard 610.12.

3.4.4

CM-Dokumentation

vollständige CM-Dokumentation, umfasst die CM-Ausgaben, die CM-Liste (Konfigurationsliste), die CM-Systemdatensätze, die CM-Planung und die CM-Nutzung

3.4.5

Konfigurationsmanagementnachweis

alle Nachweise, die verwendet werden können, um Vertrauen in den ordnungsgemäßen Betrieb des CM-Systems herzustellen

ANMERKUNG Zum Beispiel CM-Ausgaben, vom Entwickler gelieferte Begründungen, Beobachtungen, Experimente oder Interviews, die während einer Standortbegehung vom Evaluator durchgeführt wurden.

3.4.6

Konfigurationselement

Objekt, das während der TOE-Entwicklung vom CM-System gesteuert wird

ANMERKUNG Es kann sich dabei entweder um Teile des TOEs oder um Objekte handeln, die mit der Entwicklung des TOEs in Zusammenhang stehen, wie beispielsweise Beurteilungsdokumente oder Entwicklungswerkzeuge. CM-Elemente können, zusammen mit ihrer Version, entweder direkt im CM-System gespeichert sein (zum Beispiel Dateien) oder referenziert werden (zum Beispiel Hardware-Bauteile).

3.4.7

Konfigurationsliste

Ausgabedokument des Konfigurationsmanagements, das alle Konfigurationselemente für ein spezifisches Produkt zusammen mit der genauen Version aller Konfigurationsmanagementelemente auflistet, die für eine bestimmte Version des Gesamtprodukts relevant sind

ANMERKUNG Diese Liste ermöglicht die Unterscheidung der Elemente, die zur evaluierten Version des Produkts gehören, von anderen Versionen dieser Elemente, die zu anderen Produktversionen gehören. Die finale Konfigurationsmanagementliste ist ein spezifisches Dokument für eine spezifische Version des spezifischen Produkts. (Bei der Liste kann es sich natürlich um ein elektronisches Dokument innerhalb eines Konfigurationsmanagement-Werkzeugs handeln. In diesem Fall kann sie als spezifischer Einblick in das System oder einen Teil des Systems angesehen werden und nicht als eine Ausgabe des Systems. Allerdings wird die Konfigurationsliste im praktischen Einsatz während einer Evaluierung vermutlich als Teil der Evaluierungsdokumentation bereitgestellt werden.) Die Konfigurationsliste definiert die Elemente, die unter die Konfigurationsmanagementanforderungen von ALC_CMC fallen.

3.4.8

Konfigurationsmanagementausgabe

Ergebnisse in Bezug auf das Konfigurationsmanagement, die vom Konfigurationsmanagementsystem erstellt oder durchgesetzt werden

ANMERKUNG Diese mit dem Konfigurationsmanagement in Zusammenhang stehenden Ergebnisse können die Form von Dokumenten haben (zum Beispiel ausgefüllte Papierformulare, Konfigurationsmanagement-Systemdatensätze, Protokolldaten, Ausdrucke und elektronische Ausgabedaten) oder von Aktionen (zum Beispiel manuelle Maßnahmen zur Erfüllung von Konfigurationsmanagementanweisungen). Beispiele für solche Konfigurationsmanagementausgaben sind Konfigurationslisten, Konfigurationsmanagementpläne und/oder das Verhalten während des Produktlebenszyklus.

3.4.9

Konfigurationsmanagementplan

Beschreibung, wie das Konfigurationsmanagementsystem für den TOE eingesetzt wird

ANMERKUNG Das Ziel bei der Erstellung eines Konfigurationsmanagementplans ist es, Mitarbeitern deutlich zu machen, welche Aufgaben zu erfüllen sind. Aus Sicht des gesamten Konfigurationsmanagementsystems kann dieser als Ausgabedokument betrachtet werden (da er möglicherweise als Teil der Anwendung des Konfigurationsmanagementsystems erstellt wird). Aus Sicht des konkreten Projekts handelt es sich um ein Anwendungsdokument, da er von den Mitgliedern des Projektteams verwendet wird, um die Schritte zu verstehen, die während des Projekts durchgeführt werden müssen. Der Konfigurationsmanagementplan beschreibt die Anwendung des Systems für das spezifische Produkt; das gleiche System kann in einem anderen Umfang für andere Produkte eingesetzt werden. Dies bedeutet, dass der Konfigurationsmanagementplan die Ausgaben des während der TOE-Entwicklung eingesetzten Konfigurationsmanagementsystems eines Unternehmens definiert und beschreibt.

3.4.10

Konfigurationsmanagementsystem

Satz von Verfahren und Werkzeugen (einschließlich deren Dokumentation), der von einem Entwickler zur Entwicklung und Wartung der Konfigurationen seiner Produkte während deren Lebenszyklus verwendet wird

ANMERKUNG Konfigurationsmanagementsysteme können über unterschiedliche Stringenz- und Funktionsgrade verfügen. Auf den höheren Stufen können Konfigurationsmanagementsysteme automatisiert sein und über Mängelbehebung, Änderungskontrolle und andere Nachverfolgungsmechanismen verfügen.

3.4.11

Konfigurationsmanagementsystem-Datensätze

Ausgaben, die während des Betriebs des Konfigurationsmanagementsystems erstellt werden und wichtige Konfigurationsmanagementaktivitäten dokumentieren

ANMERKUNG Beispiele für Konfigurationsmanagementsystem-Datensätze sind Kontrollformulare für Änderungen der Konfigurationsmanagementsysteme oder Zugriffsgenehmigungsformulare für Konfigurationsmanagementsysteme.

3.4.12

Konfigurationsmanagementwerkzeuge

manuell geführte oder automatisierte Werkzeuge, die ein Konfigurationsmanagementsystem realisieren oder unterstützen

ANMERKUNG Beispielsweise Werkzeuge für die Versionsverwaltung der TOE-Teile.

3.4.13

Konfigurationsmanagement-Nutzungsdokumentation

Teil des Konfigurationsmanagementsystems, der beschreibt, wie das Konfigurationsmanagementsystem definiert und angewendet wird, beispielsweise mithilfe von Handbüchern, Vorschriften und/oder der Dokumentation von Werkzeugen und Verfahren

3.4.14

Auslieferung

Übergabe des fertiggestellten TOE von der Produktionsumgebung in die Hände des Kunden

ANMERKUNG Diese Produktlebenszyklusphase kann die Verpackung und Lagerung am Entwicklungsstandort beinhalten, aber umfasst nicht den Transport des nicht fertiggestellten TOE oder von dessen Teilen zwischen verschiedenen Entwicklern oder Entwicklungsstandorten.

3.4.15

Entwickler

für die Entwicklung des TOEs zuständige Organisation

3.4.16

Entwicklung

Produktlebenszyklusphase, welche die Erzeugung der Implementierungsrepräsentation des TOEs betrifft

ANMERKUNG Im Rahmen der Unterstützungsanforderungen während des ALC: Produktlebenszyklus sind Entwicklung und verwandte Begriffe (Entwickler, entwickeln) im allgemeineren Sinn zu verstehen und umfassen die Entwicklung und die Erstellung.

3.4.17

Entwicklungswerkzeuge

Werkzeuge (einschließlich Testsoftware, falls zutreffend), welche die Entwicklung und Erstellung des TOEs unterstützen

ANMERKUNG Beispielsweise sind bei einem Software-TOE die Entwicklungswerkzeuge in der Regel Programmiersprachen, Compiler, Linker und Generierungswerkzeuge.

3.4.18

Implementierungsrepräsentation

am wenigsten abstrakte Darstellung des TSF, genauer die Darstellung, die ohne weitere Designverfeinerung zur Erstellung des TSF selbst verwendet wird

ANMERKUNG Beispiele für Teile von Implementierungsrepräsentationen sind Quellcode, der anschließend kompiliert wird, oder Hardware-Zeichnungen, die zum Aufbau der eigentlichen Hardware verwendet werden.

3.4.19

Lebenszyklus

Abfolge von Daseinsstufen eines Objekts (zum Beispiel eines Produkts oder eines Systems) über die Zeit

3.4.20

Lebenszyklusdefinition

Definition des Lebenszyklusmodells

3.4.21

Lebenszyklusmodell

Beschreibung der für die Lebenszyklusverwaltung eines bestimmten Objekts verwendeten Stufen und deren Beziehungen untereinander und ihrer Abfolge sowie ein Überblick ihrer Merkmale

ANMERKUNG Siehe auch Bild 1.

3.4.22

Erstellung

die Erstellungs-Lebenszyklusphase folgt der Entwicklungsphase und besteht aus der Umsetzung der Implementierungsrepräsentation in die Implementierung des TOEs, d. h. in einen Zustand, der für die Auslieferung an den Kunden geeignet ist

ANMERKUNG Diese Phase kann die Herstellung, Integration, Generierung, interne Transporte, Lagerung und die Kennzeichnung des TOEs umfassen.

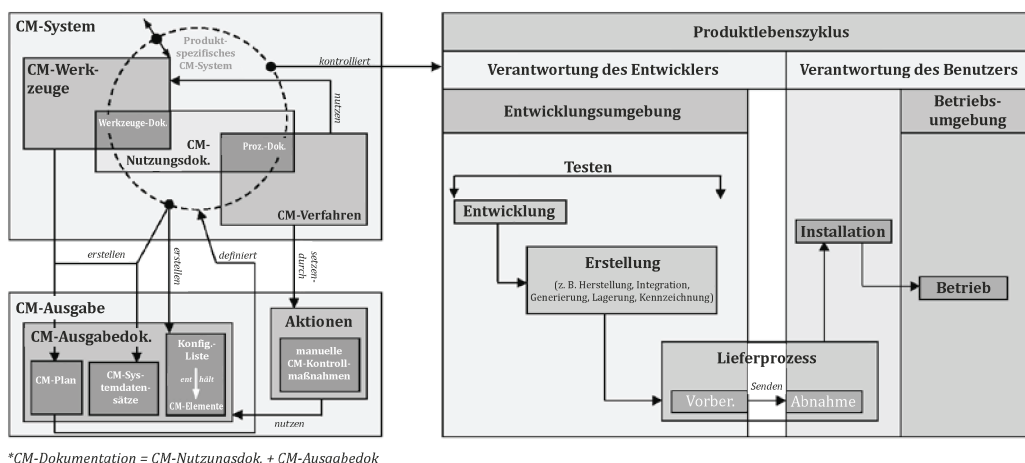


Bild 1 — Terminologie im CM und Produktlebenszyklus

3.5 Begriffe in Zusammenhang mit der Klasse AVA

3.5.1

verdeckter Kanal

erzwungener, unrechtmäßiger Signalkanal, mit dem der Benutzer heimlich die Mehrstufentrennungspolitik und die Anforderungen an die Nichtbeobachtbarkeit des TOEs umgehen kann

3.5.2

aufgedeckte mögliche Anfälligkeiten

mögliche Schwachstellen im TOE, die vom Evaluator bei der Durchführung der Evaluierungsaktivitäten identifiziert wurden und die für Verletzungen von SFRs genutzt werden könnten

3.5.3

ausnutzbare Anfälligkeit

Schwachstelle im TOE, die für Verletzungen von SFRs in der Betriebsumgebung des TOEs genutzt werden kann

3.5.4

Überwachungsangriffe

generische Angriffsmethodenkategorie, die passive Analysetechniken einschließt, welche auf die Offenlegung sensibler interner Daten des TOEs abzielen, wobei der TOE entsprechend der Leitliniendokumentation betrieben wird

3.5.5

mögliche Anfälligkeit

vermutete, aber nicht bestätigte Schwachstelle

ANMERKUNG Der Verdacht ergibt sich aufgrund eines angenommenen Angriffspfads zur Verletzung der SFRs.

3.5.6

Restanfälligkeit

Schwachstelle, die nicht in der Betriebsumgebung des TOEs ausgenutzt werden kann, die aber für Verletzungen der SFRs durch einen Angreifer genutzt werden könnte, der ein höheres Angriffspotential hat, als es für die Betriebsumgebung des TOEs angenommen wird

3.5.7

Anfälligkeit

Schwachstelle im TOE, die für Verletzungen von SFRs in manchen Umgebungen ausgenutzt werden kann

3.6 Begriffe in Zusammenhang mit der Klasse ACO

3.6.1

Basiskomponente

Entität in einem zusammengesetzten TOE, die selbst einer Evaluierung unterzogen wurde und die Dienste und Ressourcen für eine abhängige Komponente bereitstellt

3.6.2

kompatibel (Komponenten)

Eigenschaft einer Komponente, um die von einer anderen Komponente geforderten Dienste über die entsprechenden Schnittstellen der beiden Komponenten in einer konsistenten Betriebsumgebung bereitzustellen

3.6.3

Komponenten-TOE

erfolgreich bewerteter TOE, der Teil eines anderen zusammengesetzten TOEs ist

3.6.4

zusammengesetzter TOE

TOE, das nur aus zwei oder mehreren Komponenten besteht, die erfolgreich evaluiert wurden

3.6.5

abhängige Komponente

Entität in einem zusammengesetzten TOE, die selbst einer Evaluierung unterzogen wird und die auf die Bereitstellung von Diensten durch eine Basiskomponente angewiesen ist

3.6.6

funktionelle Schnittstelle

externe Schnittstelle, die dem Benutzer den Zugriff auf die Funktionalität des TOEs ermöglicht und die nicht direkt an der Durchsetzung der funktionellen Sicherheitsanforderungen beteiligt ist

ANMERKUNG In einem zusammengesetzten TOE sind dies die von der Basiskomponente bereitgestellten Schnittstellen, die von der abhängigen Komponente benötigt werden, um den Betrieb des zusammengesetzten TOEs zu unterstützen.

4 Symbole und Abkürzungen

Die folgenden Abkürzungen werden in einem oder mehreren Teilen von ISO/IEC 15408 verwendet:

API	Programmierschnittstelle (en: Application Programming Interface)
CAP	Zusammengesetztes Sicherheitspaket (en: Composed Assurance Package)
CM	Konfigurationsmanagement (en: Configuration Management)
DAC	Diskrete Zugriffskontrolle (en: Discretionary Access Control)
EAL	Vertrauenswürdigkeitsstufe (en: Evaluation Assurance Level)
GHz	Gigahertz
GUI	Grafische Benutzungsschnittstelle (en: Graphical User Interface)
IC	Integrierte Schaltung (en: Integrated Circuit)
IOCTL	Eingabe-Ausgabe-Steuerung (en: Input Output Control)
IP	Internet-Protokoll (en: Internet Protocol)
IT	Informationstechnik (en: Information Technology)
MB	Megabyte
OS	Betriebssystem (en: Operating System)
OSP	Organisatorische Sicherheitspolitik (en: Organisational Security Policy)
PC	Personal Computer
PCI	Peripheral Component Interconnect
PKI	Public-Key-Infrastruktur (en: Public Key Infrastructure)

PP	Schutzprofil (en: Protection Profile)
RAM	Direktzugriffsspeicher (en: Random Access Memory)
RPC	Remote Procedure Call
SAR	Vertrauenswürdigkeitsanforderung (en: Security Assurance Requirement)
SFR	Sicherheitsfunktionsanforderung (en: Security Functional Requirement)
SFP	Sicherheitsfunktionspolitik (en: Security Function Policy)
SPD	Sicherheitsproblemdefinition (en: Security Problem Definition)
ST	Sicherheitsvorgabe (en: Security Target)
TCP	Transmission Control Protocol
TOE	Evaluierungsgegenstand (en: Target of Evaluation)
TSF	TOE-Sicherheitsfunktionalität (en: TOE Security Functionality)
TSFI	TSF-Schnittstelle (en: TSF Interface)
VPN	Virtual Private Network

5 Übersicht

5.1 Allgemein

In diesem Abschnitt werden die wesentlichen Konzepte der ISO/IEC 15408 eingeführt. Beschrieben werden das Konzept „TOE“, die Zielgruppe der ISO/IEC 15408 und die Art der Präsentation des Inhalts der übrigen Teile der ISO/IEC 15408.

5.2 Der Evaluierungsgegenstand (TOE)

Die ISO/IEC 15408 ist flexibel bei der Frage, was evaluiert werden kann und daher nicht an die Grenzen von IT-Produkten gebunden wie sie im Allgemeinen aufgefasst werden. Daher benutzt die ISO/IEC 15408 im Zusammenhang mit der Evaluierung den Begriff „Evaluierungsgegenstand“ (TOE; en: Target of Evaluation).

Ein TOE ist ein Satz von Software, Firmware und/oder Hardware, möglicherweise mit beigefügten Leitlinien.

Der TOE mag in vielen Fällen ein IT-Produkt sein, braucht es aber nicht. Der TOE kann ein IT-Produkt sein, Teil eines IT-Produkts, ein Satz von IT-Produkten, eine spezifische Technologie, die vielleicht nie zu einem Produkt wird, oder eine Kombination dieser Komponenten.

Im Sinne der ISO/IEC 15408 ist die genaue Beziehung zwischen dem TOE und jeglichem IT-Produkt nur für einen Aspekt wichtig: Die Evaluierung eines TOEs, das nur einen Teil des IT-Produkts umfasst, sollte nicht fälschlich für die Evaluierung des gesamten IT-Produkts gehalten werden.

Beispiele für TOEs sind:

- eine Softwareanwendung;
- ein Betriebssystem;

- eine Softwareanwendung in Verbindung mit einem Betriebssystem;
- eine Softwareanwendung in Verbindung mit einem Betriebssystem und einer Arbeitsstation;
- ein Betriebssystem in Verbindung mit einer Arbeitsstation;
- eine Chipkarte mit integrierter Schaltung;
- der kryptographische Co-Prozessor einer Chipkarte mit integrierter Schaltung;
- ein lokales Netz (LAN) mit allen Terminals, Servern, Netzwerkeinrichtungen und Software;
- eine Datenbankanwendung ohne Remote-Client-Software, die bei Datenbankanwendungen üblich ist.

5.2.1 Unterschiedliche Darstellungen des TOEs

In der ISO/IEC 15408 kann ein TOE in unterschiedlichen Darstellungen auftreten, beispielsweise (bei einem Software-TOE):

- eine Liste von Dateien in einem Konfigurationsmanagementsystem;
- eine einzige Master-Kopie, die soeben kompiliert wurde;
- eine Schachtel mit einer CD-ROM und einem Handbuch, bereit zur Lieferung an den Kunden;
- eine installierte und betriebsbereite Version.

Alle Aufzählungspunkte werden als TOE betrachtet und überall, wo der Begriff „TOE“ in einem weiteren Teil der ISO/IEC 15408 verwendet wird, bestimmt der Kontext die angedachte Darstellung.

5.2.2 Unterschiedliche Konfigurationen des TOEs

Im Allgemeinen können IT-Produkte auf unterschiedliche Weise konfiguriert werden: unterschiedliche Arten der Installation, mit verschiedenen aktivierten oder deaktivierten Optionen. Während einer Evaluierung nach ISO/IEC 15408 wird bestimmt, ob ein TOE gewisse Anforderungen erfüllt; dadurch kann diese Flexibilität in der Konfiguration zu Problemen führen, da alle möglichen Konfigurationen des TOEs die Anforderungen erfüllen müssen. Daher ist es häufig der Fall, dass der Leitlinien-Teil des TOEs die möglichen Konfigurationen stark einschränkt. Das heißt: Die Leitlinien des TOEs dürfen sich von den allgemeinen Leitlinien des IT-Produkts unterscheiden.

Ein Beispiel ist ein IT-Produkt vom Typ Betriebssystem. Das Produkt kann auf verschiedene Arten konfiguriert werden (z. B. Arten der Benutzer, Anzahl der Benutzer, Arten der erlaubten/unerlaubten externen Verbindungen, aktivierte/deaktivierte Optionen usw.).

Wenn dasselbe IT-Produkt ein TOE sein soll und gegen eine erhebliche Reihe an Anforderungen evaluiert wird, sollte die Konfiguration sehr viel enger kontrolliert werden, da viele Optionen (z. B.: Erlauben aller Arten von externen Verbindungen oder keine Pflicht zur Authentifizierung des Systemadministrators) dazu führen werden, dass der TOE die Anforderungen nicht erfüllt.

Daher wird es üblicherweise einen Unterschied zwischen den Leitlinien des IT-Produkts (erlaubt viele Konfigurationen) und den Leitlinien des TOEs geben (erlaubt nur eine Konfiguration oder nur Konfigurationen, die in sicherheitsbezogenen Punkten nicht abweichen).

Es ist zu beachten, dass, wenn die Leitlinien des TOEs noch mehr als eine Konfiguration erlauben, diese Konfigurationen insgesamt „der TOE“ genannt werden, und jede einzelne Konfiguration die an den TOE gestellten Anforderungen erfüllen muss.

5.3 Zielgruppe der ISO/IEC 15408

Drei Gruppen haben ein allgemeines Interesse an der Evaluierung der Sicherheitseigenschaften von TOEs: Verbraucher, Entwickler und Evaluatoren. Die in der ISO/IEC 15408 Teil 1 dargelegten Kriterien sind so strukturiert, dass sie die Bedürfnisse aller drei Gruppen abdecken. Sie alle gelten als wesentliche Anwender der ISO/IEC 15408. In den folgenden Absätzen wird erklärt, wie die drei Gruppen von den Kriterien profitieren können.

5.3.1 Verbraucher

Die ISO/IEC 15408 wurde geschrieben, um sicherzustellen, dass die Evaluierung die Bedürfnisse der Verbraucher erfüllt, da dies grundlegender Zweck und Grund für den Evaluierungsprozess ist.

Verbraucher können die Ergebnisse der Evaluierung als Hilfe bei der Entscheidung verwenden, ob ein TOE ihre Sicherheitsbedürfnisse erfüllt. Diese Sicherheitsbedürfnisse sind üblicherweise das Ergebnis einer Risikoanalyse und auch der Ausrichtung einer Richtlinie. Verbraucher können die Evaluierungsergebnisse auch verwenden, um verschiedene TOEs zu vergleichen.

Die ISO/IEC 15408 übergibt Verbrauchern, insbesondere Verbrauchergruppen und Interessengemeinschaften, eine implementationsunabhängige Struktur, dem Schutzprofil (PP; en: protection profile), in dem ihre Sicherheitsanforderungen eindeutig formuliert werden können.

5.3.2 Entwickler

Die ISO/IEC 15408 ist für die Unterstützung von Entwicklern ausgelegt und bereitet sie auf die Evaluierung der TOEs vor und hilft beim Identifizieren der von den TOEs zu erfüllenden Sicherheitsanforderungen. Diese Anforderungen sind in einem implementationsabhängigen Konstrukt, der Sicherheitsvorgabe (ST; en: security target) enthalten. Diese ST kann auf einem oder mehreren PPs basieren, um aufzuzeigen, dass die ST den Sicherheitsanforderungen von Verbrauchern entspricht, die in jenen PPs dargelegt sind.

Die ISO/IEC 15408 kann anschließend zur Bestimmung der Verantwortlichkeiten und Aktionen verwendet werden, um bei der Erbringung der erforderlichen Nachweise zur Evaluierung des TOEs gegen diese Anforderung zu unterstützen. Die Norm definiert außerdem den Inhalt und die Präsentation dieser Nachweise.

5.3.3 Evaluatoren

Die ISO/IEC 15408 enthält Kriterien, die von Evaluatoren bei ihrer Beurteilung zur Konformität von TOEs mit ihren Sicherheitsanforderungen zu verwenden sind. Die ISO/IEC 15408 beschreibt eine Reihe von allgemeinen Aktionen, die von Evaluatoren auszuführen sind. Es ist zu beachten, dass die ISO/IEC 15408 keine Verfahren zur Ausführung dieser Aktionen spezifiziert. Weitere Informationen zu diesen Verfahren finden sich in 5.5.

5.3.4 Weitere

Die ISO/IEC 15408 ist zwar für die Spezifizierung und Evaluierung von IT-Sicherheitseigenschaften von TOEs ausgelegt, kann aber auch als Verweismaterial für alle interessierten oder verantwortlichen Parteien in der IT-Sicherheit nützlich sein. Einige der zusätzlichen Interessengruppen, die von den in der ISO/IEC 15408 enthaltenen Informationen profitieren können, sind:

- a) Systemverwalter und Systemsicherheitsbeauftragte, die für die Bestimmung und Einhaltung organisatorischer IT-Sicherheitsrichtlinien und Sicherheitsanforderungen verantwortlich sind;
- b) Auditoren, sowohl interne als auch externe, die für die Bewertung der Angemessenheit der Sicherheit einer IT-Lösung (die ein TOE sein oder enthalten kann) verantwortlich sind;
- c) Sicherheitsarchitekten und Sicherheitsdesigner, die für die Spezifizierung der Sicherheitseigenschaften eines IT-Produkts verantwortlich sind;

- d) Akkreditierer, die für das Akzeptieren einer IT-Lösung zur Verwendung in einer bestimmten Umgebung verantwortlich sind;
- e) Sponsoren der Evaluierung, die für die Anforderung und Unterstützung einer Evaluierung verantwortlich sind; und
- f) Evaluierungsinstanzen, die für das Management und die Aufsicht eines IT-Sicherheitsevaluierungsprogramms verantwortlich sind.

5.4 Die verschiedenen Teile der ISO/IEC 15408

Wie unten aufgezeigt, wird die ISO/IEC 15408 als eine Reihe eigenständiger aber zusammenhängender Teile dargestellt. In der Beschreibung der Teile verwendete Begriffe werden in Abschnitt 6 erklärt.

- a) **Teil 1, Einleitung und allgemeines Modell** ist die Einleitung zur ISO/IEC 15408. Dieser Teil definiert die allgemeinen Konzepte und Grundlagen der IT-Sicherheitsevaluierung und zeigt ein allgemeines Evaluierungsmodell.
- b) **Teil 2, Sicherheitsfunktionskomponenten** legt einen Satz an Funktionskomponenten als Standardvorlagen fest, die als Grundlage für funktionale Anforderungen an TOEs dienen. ISO/IEC 15408-2 katalogisiert den Satz an Funktionskomponenten und organisiert ihn in Familien und Klassen.
- c) **Teil 3, Vertrauenswürdigkeitskomponenten** legt einen Satz an Vertrauenswürdigkeitskomponenten als Standardvorlagen fest, die als Grundlage für Vertrauenswürdigkeitsanforderungen an TOEs dienen. ISO/IEC 15408-3 katalogisiert den Satz an Vertrauenswürdigkeitskomponenten und organisiert ihn in Familien und Klassen. Die ISO/IEC 15408-3 definiert außerdem die Evaluierungskriterien für PPs und STs und zeigt sieben vordefinierte Sicherheitspakete, die als Vertrauenswürdigkeitsstufen (EAL-Stufen) bezeichnet werden.

Zur Unterstützung der o. a. drei Teile der ISO/IEC 15408 wurden noch weitere Dokumente veröffentlicht. Die ISO/IEC 18045 umfasst beispielsweise die Methodologie für die IT-Sicherheitsevaluierung auf Grundlage der ISO/IEC 15408. Die Veröffentlichung weiterer Dokumente wird erwartet, darunter technische Begründungen und Leitliniendokumente.

Folgende Tabelle zeigt, wie die Teile der ISO/IEC 15408 für die drei wesentlichen Zielgruppen von Interesse sein können.

Tabelle 1 — Roadmap für die „Evaluierungskriterien für IT-Sicherheit“

	Verbraucher	Entwickler	Evaluatoren
Teil 1	Verwendung als Hintergrundinformation und verpflichtend für Verweisungszwecke. Leitfadenstruktur für PPs.	Verwendung als Hintergrundinformation und für Verweisungszwecke. Verpflichtend für die Entwicklung von Sicherheitsspezifikationen für TOEs.	Verpflichtend für Verweisungszwecke und als Leitfaden für die Struktur von PPs und STs.
Teil 2	Verwendung als Leitfaden und zur Verweisung bei der Festlegung von Aussagen zu Anforderungen für ein TOE.	Verpflichtend zur Verweisung bei der Interpretation von Aussagen zu funktionalen Anforderungen und bei der Formulierung von funktionalen Spezifikationen für TOEs.	Verpflichtend zur Verweisung bei der Interpretation von Aussagen zu funktionalen Anforderungen.
Teil 3	Verwendung als Leitfaden bei der Bestimmung der erforderlichen Sicherheitsstufen.	Verwendung als Verweisung bei der Interpretation von Aussagen zu Sicherheitsanforderungen und bei der Bestimmung von Sicherheitskonzepten für TOEs.	Verwendung als Verweisung bei der Interpretation von Aussagen zu Sicherheitsanforderungen.

5.5 Evaluierungskontext

Um eine bessere Vergleichbarkeit zwischen den Evaluierungsergebnissen zu erreichen, sollten die Evaluierungen innerhalb des Rahmenwerks eines verbindlichen Evaluierungsplans ausgeführt werden, der die Standards festlegt, die Qualität der Evaluierungen überwacht und die Einhaltung der Vorschriften an die Evaluierungseinrichtungen und Evaluatoren verwaltet.

Die ISO/IEC 15408 enthält keine Aussagen zum regulatorischen Rahmenwerk. Eine Konsistenz zwischen den regulatorischen Regelwerken der verschiedenen Evaluierungsinstanzen ist allerdings erforderlich, um das Ziel einer gegenseitigen Anerkennung der Ergebnisse solcher Evaluierungen zu erreichen.

Ein zweiter Weg zum Erreichen einer besseren Vergleichbarkeit der Evaluierungsergebnisse besteht in der Verwendung einer einheitlichen Methodologie zum Erreichen dieser Ergebnisse. Für die ISO/IEC 15408 ist diese Methodologie in der ISO/IEC 18045 enthalten.

Die Verwendung einer einheitlichen Evaluierungsmethodologie trägt zur Wiederholbarkeit und Objektivität der Ergebnisse bei, ist aber für sich genommen nicht ausreichend. Eine Vielzahl der Evaluierungskriterien erfordert die Beurteilung durch Experten und Hintergrundwissen; hierfür ist Konsistenz schwieriger zu erreichen. Um die Konsistenz von Evaluierungsfeststellungen zu verbessern, dürfen die finalen Evaluierungsergebnisse an einen Zertifizierungsprozess übergeben werden.

Der Zertifizierungsprozess ist die unabhängige Prüfung der Evaluierungsergebnisse und führt zur Erstellung des finalen Zertifikats oder der finalen Genehmigung, die üblicherweise öffentlich verfügbar sind. Der Zertifizierungsprozess ist ein Mittel zum Erreichen von besserer Vergleichbarkeit in der Anwendung der IT-Sicherheitskriterien.

Die Evaluierungspläne und Zertifizierungsprozesse liegen in der Verantwortung der Evaluierungsinstanzen, die solche Pläne und Prozesse betreiben, und sind daher außerhalb des Anwendungsbereichs der ISO/IEC 15408.

6 Allgemeines Modell

6.1 Einführung in das allgemeine Modell

Dieser Abschnitt zeigt die durchgängig in der ISO/IEC 15408 verwendeten allgemeinen Konzepte, einschließlich des Kontextes, in dem die Konzepte für die ISO/IEC 15408 zu verwenden sind, und des Ansatzes zur Anwendung der Konzepte. Anwender dieses Teils der ISO/IEC 15408 sind außerdem verpflichtet, die ISO/IEC 15408-2 und die ISO/IEC 15408-3 zu verwenden, da sie die Verwendung der Konzepte weiter ausführen und davon ausgehen, dass der beschriebene Ansatz verfolgt wird. Des Weiteren ist die ISO/IEC 18045 anwendbar für Anwender der ISO/IEC 15408, die Evaluierungstätigkeiten planen. Dieser Abschnitt setzt gewisse Vorkenntnisse in der IT-Sicherheit voraus und ist nicht als ein Tutorium für diesen Bereich ausgelegt.

Die ISO/IEC 15408 behandelt Sicherheit über eine Reihe von Sicherheitskonzepten und Terminologie. Ein Verständnis dieser Konzepte und der Terminologie ist eine Voraussetzung für die effektive Verwendung der ISO/IEC 15408. Die Konzepte selbst sind allerdings recht allgemein gehalten und nicht dazu ausgelegt, die Klassen der IT-Sicherheitsprobleme einzuschränken, für die ISO/IEC 15408 anwendbar ist.

6.2 Vermögenswerte und Gegenmaßnahmen

Bei der Sicherheit geht es um den Schutz von Vermögenswerten. Vermögenswerte sind Einheiten, in denen jemand einen Wert sieht. Beispiele für Vermögenswerte sind:

- Inhalte von Dateien oder eines Servers;
- die Authentizität von abgegebenen Stimmen in einer Wahl;
- die Verfügbarkeit eines elektronischen Handelsprozesses;
- die Möglichkeit, einen hochpreisigen Drucker zu verwenden;
- Zutritt zu einer als vertraulich eingestuften Einrichtung.

Da Wert allerdings äußerst subjektiv ist, kann beinahe alles ein Vermögenswert sein.

Die Umgebungen dieser Vermögenswerte werden Betriebsumgebung genannt. Beispiele für (Aspekte einer) Betriebsumgebung sind:

- der Rechnerraum einer Bank;
- ein Rechnernetzwerk, das mit dem Internet verbunden ist;
- ein lokales Netz;
- eine allgemeine Büroumgebung.

Viele Vermögenswerte liegen in der Form von Informationen vor, die von IT-Produkten gespeichert, verarbeitet und übertragen werden, welche die von den Informationseigentümern festgelegten Anforderungen erfüllen müssen. Informationseigentümer können verlangen, dass Verfügbarkeit, Verbreitung und Veränderung solcher Informationen streng geregelt sind und dass Vermögenswerte durch Gegenmaßnahmen vor Bedrohungen geschützt werden. Bild 2 zeigt diese übergeordneten Konzepte und Beziehungen.

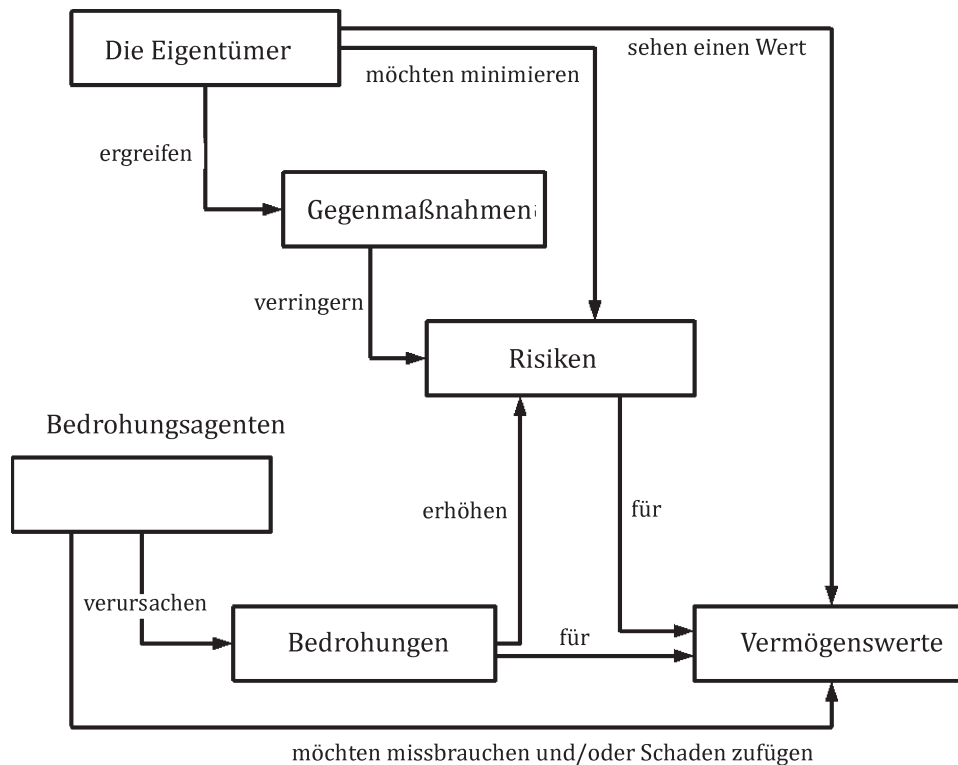


Bild 2 — Sicherheitskonzepte und Beziehungen

Die Absicherung von Vermögenswerten liegt in der Verantwortung der Eigentümer, die Wert in diesen Vermögenswerten sehen. Tatsächliche und angenommene Bedrohungsagenten können auch Wert in den Vermögenswerten sehen und versuchen, diese Vermögenswerte in einem dem Eigentümer entgegengesetztem Interesse zu missbrauchen. Beispiele für Bedrohungsagenten umfassen Hacker, böswillige Benutzer, nicht-böswillige Benutzer (die manchmal Fehler machen), Computerprozesse und Unfälle.

Die Eigentümer der Vermögenswerte sehen diese Bedrohungen insofern als ein Potential zur Schädigung ihrer Vermögenswerte, da der Wert der Vermögenswerte der Eigentümer reduziert würde. Sicherheitsspezifische Schädigung umfasst häufig, aber ist nicht beschränkt auf den Verlust der Vertraulichkeit des Vermögenswerts, den Verlust der Integrität des Vermögenswerts und den Verlust der Verfügbarkeit des Vermögenswerts.

Diese Bedrohungen verursachen daher Risiken für die Vermögenswerte, basierend auf der Wahrscheinlichkeit der Umsetzung der Bedrohung und des Einflusses auf die Vermögenswerte, wenn die Bedrohung umgesetzt wird. Anschließend werden Gegenmaßnahmen ergriffen, um die Risiken auf die Vermögenswerte zu reduzieren. Diese Gegenmaßnahmen können IT-Gegenmaßnahmen (wie Firewalls und Chipkarten) und Nicht-IT-Gegenmaßnahmen (wie Wachleute und Verfahren) umfassen. Siehe auch ISO/IEC 27001 und ISO/IEC 27002 für eine allgemeinere Erörterung zu Sicherheitsgegenmaßnahmen (Kontrollen) und zur Implementierung und Verwaltung von Gegenmaßnahmen.

Eigentümer von Vermögenswerten können verantwortlich (oder haftbar) sein für diese Vermögenswerte und sollten daher in der Lage sein, die Entscheidung zum Akzeptieren der Risiken zu verteidigen, wenn die Vermögenswerte den Bedrohungen ausgesetzt werden.

Bei der Verteidigung dieser Entscheidung gibt es zwei wichtige Elemente, die das demonstrieren:

- die Gegenmaßnahmen sind *angemessen*: wenn die Gegenmaßnahmen das tun, was sie versprechen, sind die Bedrohungen für die Vermögenswerte abgewehrt;
- die Gegenmaßnahmen sind *korrekt*: die Gegenmaßnahmen tun, was sie versprechen.

Vielen Eigentümern von Vermögenswerten mangelt es an Wissen, Expertise oder den erforderlichen Ressourcen, um die Angemessenheit und die Korrektheit der Gegenmaßnahmen zu beurteilen, und die Eigentümer möchten sich möglicherweise nicht allein auf die Aussagen der Entwickler der Gegenmaßnahmen verlassen. Diese Verbraucher können sich daher dazu entschließen, ihre Zuversicht in Angemessenheit und Korrektheit einiger oder aller derer Gegenmaßnahmen zu erhöhen, indem sie eine Evaluierung dieser Gegenmaßnahmen beauftragen.

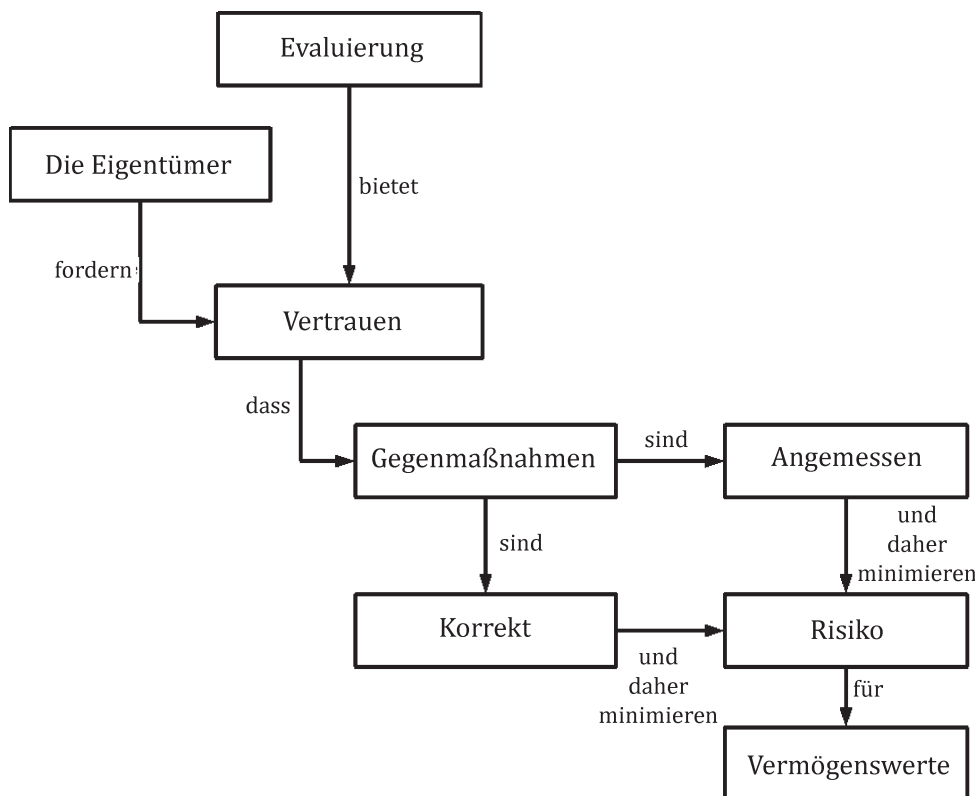


Bild 3 — Evaluierungskonzepte und Beziehungen

6.2.1 Angemessenheit der Gegenmaßnahmen

Die Angemessenheit der Gegenmaßnahmen wird bei einer Evaluierung über ein Konstrukt namens Sicherheitsvorgabe analysiert. Dieser Unterabschnitt bietet eine vereinfachte Sicht auf dieses Konstrukt: eine detailliertere und vollständige Beschreibung findet sich in Anhang A.

Die Sicherheitsvorgabe beginnt mit der Beschreibung der Vermögenswerte und ihrer Bedrohungen. Die Sicherheitsvorgabe beschreibt anschließend die Gegenmaßnahmen (in Form von Sicherheitszielsetzungen) und demonstriert, dass diese Gegenmaßnahmen angemessen sind, um diese Bedrohungen abzuwehren: wenn die Gegenmaßnahmen das tun, was sie versprechen, werden die Bedrohungen abgewehrt.

Anschließend teilt die Sicherheitsvorgabe diese Gegenmaßnahmen in zwei Gruppen ein:

- die Sicherheitszielsetzungen für den TOE: diese beschreiben die Gegenmaßnahme(n), für die in der Evaluierung Korrektheit bestimmt wird;
- die Sicherheitszielsetzungen für die Betriebsumgebung: diese beschreiben die Gegenmaßnahmen, für die in der Evaluierung Korrektheit nicht bestimmt wird.

Die Gründe für diese Einteilung sind wie folgt.

- Die ISO/IEC 15408 ist nur geeignet für die Bewertung der Korrektheit von IT-Gegenmaßnahmen. Daher sind Nicht-IT-Gegenmaßnahmen (z. B. Wachleute, Verfahren) immer Teil der Betriebsumgebung.
- Die Bewertung der Korrektheit von Gegenmaßnahmen kostet Zeit und Geld und die Bewertung aller IT-Gegenmaßnahmen ist daher vermutlich unzumutbar.
- Die Korrektheit einiger IT-Gegenmaßnahmen wurde vielleicht auch bereits in einer anderen Evaluierung bewertet. Daher ist es nicht wirtschaftlich, diese Korrektheit erneut zu bewerten.

Für einen TOE (die IT-Gegenmaßnahmen, deren Korrektheit in der Evaluierung bewertet werden) erfordert die Sicherheitsvorgabe eine weitere Detaillierung der Sicherheitszielsetzungen für den TOE in Sicherheitsfunktionsanforderungen (SFRs; en: security functional requirements). Diese SFRs werden in einer standardisierten Sprache formuliert (beschrieben in ISO/IEC 15408-2), um Genauigkeit sicherzustellen und Vergleichbarkeit herzustellen.

Zusammengefasst demonstrieren die Sicherheitsvorgaben Folgendes:

- die SFRs erfüllen die Sicherheitszielsetzungen für den TOE;
- die Sicherheitszielsetzungen für den TOE und die Sicherheitszielsetzungen für die Betriebsumgebung wehren die Bedrohungen ab;
- und deshalb wehren die SFRs und die Sicherheitszielsetzungen für die Betriebsumgebung die Bedrohungen ab.

Daraus folgt, dass ein korrekter TOE (der die SFRs erfüllt) in Verbindung mit einer korrekten Betriebsumgebung (die die Sicherheitszielsetzungen für diese Betriebsumgebung erfüllt) die Bedrohungen abwehren wird. Die Korrektheit des TOEs und die Korrektheit der Betriebsumgebung werden in den beiden folgenden Unterabschnitten separat erörtert.

6.2.2 Korrektheit des TOEs

Ein TOE kann inkorrekt gestaltet oder implementiert sein und daher Fehler enthalten, die zu Schwachstellen führen. Durch das Ausnutzen dieser Schwachstellen können Angreifer die Vermögenswerte beschädigen und/oder missbrauchen.

Ursachen für diese Schwachstellen können unabsichtliche Fehler in der Entwicklung, schlechtes Design, absichtliches Hinzufügen von Schadcode, unzureichende Prüfungen usw. sein.

Um die Korrektheit des TOEs zu bestimmen, können unterschiedliche Tätigkeiten ausgeführt werden, beispielsweise:

- Prüfen des TOEs;
- Untersuchen unterschiedlicher Design-Darstellungen des TOEs;
- Untersuchen der physischen Sicherheit der Entwicklungsumgebung des TOEs.

Die Sicherheitsvorgabe bietet eine strukturierte Beschreibung dieser Tätigkeiten zur Bestimmung der Korrektheit in Form von Vertrauenswürdigkeitsanforderungen (SARs; en: security assurance requirements). Diese SARs werden in einer standardisierten Sprache formuliert (beschrieben in ISO/IEC 15408-3), um Genauigkeit sicherzustellen und Vergleichbarkeit herzustellen.

Wenn die SARs erfüllt werden, besteht die Zusicherung der Korrektheit des TOEs und es ist daher unwahrscheinlicher, dass der TOE Schwachstellen enthält, die von Angreifern ausgenutzt werden können. Der Grad an Vertrauenswürdigkeit in die Korrektheit des TOEs wird durch die SARs selbst bestimmt: einige „schwache“ SARs führen zu einer niedrigen Vertrauenswürdigkeit, viele „starke“ SARs führen zu einer hohen Vertrauenswürdigkeit.

6.2.3 Korrektheit der Betriebsumgebung

Auch eine Betriebsumgebung kann inkorrekt gestaltet oder implementiert sein und daher Fehler enthalten, die zu Schwachstellen führen. Durch das Ausnutzen dieser Schwachstellen können Angreifer die Vermögenswerte beschädigen und/oder missbrauchen.

Über die ISO/IEC 15408 ist allerdings keine Zusicherung zur Korrektheit der Betriebsumgebung möglich. Anders ausgedrückt: Die Betriebsumgebung wird nicht evaluiert (siehe folgenden Unterabschnitt).

In Bezug auf die Evaluierung wird davon ausgegangen, dass die Betriebsumgebung eine zu 100 % korrekte Instanziierung der Sicherheitszielsetzungen für die Betriebsumgebung ist.

Das hindert jedoch den Verbraucher des TOEs nicht daran, andere Methoden zur Bestimmung der Korrektheit seiner Betriebsumgebung zu anzuwenden, beispielsweise die Folgenden.

- Wenn für ein Betriebssystem-TOE die Sicherheitszielsetzungen für die Betriebsumgebung besagen „Die Betriebsumgebung muss sicherstellen, dass Entitäten aus einem nicht vertrauenswürdigen Netzwerk (z. B. dem Internet) nur über ftp auf den TOE zugreifen können“, so könnte der Verbraucher eine evaluierte Firewall auswählen und so konfigurieren, dass nur ftp-Zugriff auf den TOE zu erlaubt ist.
- Wenn die Sicherheitszielsetzungen für die Betriebsumgebung besagen „Die Betriebsumgebung muss sicherstellen, dass alle Administratoren sich nicht böswillig verhalten“, so könnte der Verbraucher seine Verträge mit den Administratoren um entsprechende Strafsanktionen erweitern, aber diese Bestimmung ist nicht Teil der Evaluierung nach ISO/IEC 15408.

6.3 Evaluierung

Die ISO/IEC 15408 unterscheidet zwei Arten der Evaluierung: eine ST-/TOE-Evaluierung, die weiter unten beschrieben wird, und eine Evaluierung von PPs, die in der ISO/IEC 15408-3 definiert ist. Die ISO/IEC 15408 verwendet an vielen Stellen den Begriff Evaluierung (ohne weitere Angabe) und bezieht sich damit auf eine ST-/TOE- Evaluierung.

In der ISO/IEC 15408 erfolgt eine ST-/TOE- Evaluierung in zwei Schritten:

- a) eine ST-Evaluierung, bei der die Angemessenheit des TOEs und der Betriebsumgebung bestimmt wird;
- b) eine TOE-Evaluierung, bei der Korrektheit des TOEs bestimmt wird. Wie bereits erwähnt, wird die Korrektheit der Betriebsumgebung bei der TOE-Evaluierung nicht bewertet.

Die ST-Evaluierung wird über die Anwendung der Evaluierungskriterien für die Sicherheitsvorgabe (definiert in der ISO/IEC 15408-3) auf die Sicherheitsvorgabe ausgeführt. Die genaue Methode zur Anwendung der ASE-Kriterien wird durch die verwendete Evaluierungsmethodologie vorgegeben.

Die TOE-Evaluierung ist komplexer. Die wesentlichen Inputs einer TOE-Evaluierung sind: der Evaluierungsnachweis, der den TOE und die ST enthält, aber üblicherweise auch Input aus der Entwicklungsumgebung wie Design-Dokumente oder Testergebnisse von Entwicklern.

Die TOE-Evaluierung umfasst die Anwendung der SARs (aus der Sicherheitsvorgabe) auf den Evaluierungsnachweis. Die genaue Methode zur Anwendung einer bestimmten SAR wird durch die verwendete Evaluierungsmethodologie vorgegeben.

Die Dokumentation der Ergebnisse aus der Anwendung der SARs, und welche Berichte in welchem Umfang erzeugt werden müssen, wird sowohl durch die verwendete Evaluierungsmethodologie als auch den eingesetzten Evaluierungsplan vorgegeben.

Das Ergebnis des TOE-Evaluierungsprozesses ist entweder

- eine Aussage, dass nicht alle SARs erfüllt wurden und daher die angegebene Stufe an Vertrauenswürdigkeit, dass der TOE die in der ST angegebenen SFRs erfüllt, nicht erreicht wird oder
- eine Aussage, dass alle SARs erfüllt wurden und daher die angegebene Stufe an Vertrauenswürdigkeit, dass der TOE die in der ST angegebenen SFRs erfüllt, erreicht wird.

Die TOE-Evaluierung kann nach Abschluss der TOE-Entwicklung oder zeitgleich zur TOE-Entwicklung ausgeführt werden.

Die Methode zur Angabe der ST-/TOE-Evaluierungsergebnisse ist in Abschnitt 9 beschrieben. Diese Ergebnisse bestimmen auch das/die PP(s) und das/die Paket(e), für die der TOE Konformität beansprucht; diese Konstrukte sind im folgenden Abschnitt beschrieben.

7 Anpassung von Sicherheitsanforderungen

7.1 Operationen

Die Funktionskomponenten und Sicherheitskomponenten der ISO/IEC 15408 können genauso verwendet werden, wie in der ISO/IEC 15408-2 und ISO/IEC 15408-3 definiert, oder sie können für die Verwendung zulässiger Operationen angepasst werden. Wenn Operationen verwendet werden, sollte der PP-/ST-Autor besonders darauf achten, dass die Abhängigkeiten aus anderen Anforderungen, die von dieser Anforderung abhängen, erfüllt sind. Die zulässigen Operationen werden aus folgender Menge ausgewählt:

- Iteration: erlaubt die mehrmalige Verwendung einer Komponente mit wechselnden Operationen;
- Zuweisung: erlaubt die Spezifizierung von Parametern;
- Auswahl: erlaubt die Spezifizierung von einem oder mehreren Elementen aus einer Liste; und
- Präzisierung: erlaubt das Hinzufügen von Details.

Die Operationen Zuweisung und Auswahl sind nur zulässig, wenn dies explizit in einer Komponente angezeigt wird. Iteration und Präzisierung sind für alle Operationen zulässig. Eine ausführlichere Beschreibung dieser Operationen folgt unten.

Die Anhänge der ISO/IEC 15408-2 bieten Leitlinien für die zulässige Gestaltung von Auswahlen und Zuweisungen. Diese Leitlinien enthalten normative Anleitungen zum Vervollständigen von Operationen; diese Anleitungen müssen befolgt werden, es sei denn, der PP-/ST-Autor rechtfertigt die Abweichung.

- a) „Keine“ ist nur als Option für die Vervollständigung einer Auswahl verfügbar, wenn dies explizit angeboten wird.

Die angebotenen Listen für die Vervollständigung von Auswahlen müssen „nicht-leer“ sein. Wenn die Option „Keine“ ausgewählt wird, dürfen keine anderen Optionen ausgewählt werden. Wenn „Keine“ nicht als Option in einer Auswahl verfügbar ist, dann ist es zulässig, die Optionen in einer Auswahl mit „unds“ und „oders“ zu kombinieren, es sei denn, die Auswahl gibt explizit „eine auswählen“ vor.

Auswahl-Operationen dürfen mit Iterationen kombiniert werden, falls erforderlich. In solch einem Fall sollte die Anwendbarkeit einer ausgewählten Option für jede Iteration sich nicht mit dem Inhalt einer anderen iterierten Auswahl überschneiden, da jede Auswahl exklusiv sein soll.

- b) Bei der Gestaltung von Zuweisungen müssen die Anhänge der ISO/IEC 15408-2 hinzugezogen werden, um zu bestimmen, in welchen Fällen „Keine“ eine gültige Gestaltung ist.

7.1.1 Die Operation Iteration

Die Operation Iteration darf für jede Komponente ausgeführt werden. Der Autor PP-/ST-Autor führt eine Iterationsoperation unter Einbeziehung mehrerer Anforderungen auf Grundlage der gleichen Komponente durch. Jede Iteration einer Komponente muss sich von allen anderen Iterationen dieser Komponente unterscheiden; dies wird über die unterschiedliche Ausgestaltung von Zuweisungen und Auswahlen oder durch die Anwendung von Präzisierungen umgesetzt.

Unterschiedliche Iterationen sollten eindeutig identifiziert werden, um klare Begründungen und Rückverfolgbarkeit von und zu diesen Anforderungen zu erreichen.

Es ist wichtig zu beachten, dass eine Operation vom Typ Iteration manchmal auch mit Komponenten verwendet werden kann, bei denen auch eine Operation vom Typ Zuweisung möglich ist; diese Zuweisung könnte dann einen Bereich oder eine Werteliste enthalten, anstatt die Komponente zu iterieren. In solch einem Fall kann der Autor die zweckmäßigste Alternative auswählen; dabei ist zu berücksichtigen, ob eine vollständige Begründung für den gesamten Wertebereich notwendig ist, oder ob es erforderlich ist, eine separate Begründung für jeden einzelnen Wert zu verwenden. Der Autor sollte auch beachten, ob individuelle Rückverfolgbarkeit für diese Werte erforderlich ist.

7.1.2 Die Operation Zuweisung

Eine Zuweisungsoperation tritt auf, wenn eine Komponente ein Element mit einem Parameter enthält, der von einem PP-/ST-Autor gesetzt werden kann. Der Parameter kann eine uneingeschränkte Variable oder eine Regel sein, die die Variable auf einen bestimmten Wertebereich einschränkt.

Wenn ein Element in einem PP eine Zuweisung enthält, muss ein PP-Autor eine von vier Aufgaben ausführen:

- die Zuweisung unvollständig lassen. Der PP-Autor könnte FIA_AFL.1.2 „Wenn die definierte Anzahl an nicht erfolgreichen Authentifizierungsversuchen erreicht oder überschritten wurde, muss die TSF **[Zuweisung: Maßnahmenliste]**“ im PP einschließen;
- die Zuweisung vervollständigen. Als Beispiel könnte der PP-Autor FIA_AFL.1.2 „Wenn die definierte Anzahl an nicht erfolgreichen Authentifizierungsversuchen erreicht oder überschritten wurde, muss die TSF **diese externe Entität zukünftig von der Bindung zu jeglichem Subjekt abhalten.**“ im PP einschließen;
- die Zuweisung einschränken, um den erlaubten Wertebereich weiter zu beschränken. Als Beispiel könnte der PP-Autor FIA_AFL.1.1 „Die TSF muss **feststellen, wenn [Zuweisung: positive ganze Zahl zwischen 4 und 9] nicht erfolgreiche Authentifizierungsversuche auftreten ...**“ im PP einschließen;
- die Zuweisung in eine Auswahl umwandeln und damit die Zuweisung einschränken. Als Beispiel könnte der PP-Autor FIA_AFL.1.2 „Wenn die definierte Anzahl an nicht erfolgreichen Authentifizierungsversuchen erreicht oder überschritten wurde, muss die TSF **[Auswahl: diesen Benutzer zukünftig von der Bindung zu jeglichem Subjekt abhalten, den Administrator benachrichtigen].**“ im PP einschließen.

Wenn ein Element in einer ST eine Zuweisung enthält, muss ein ST-Autor die Zuweisung wie oben in b) vervollständigen. Optionen a), c) und d) sind für STs nicht erlaubt.

Die ausgewählten Werte in den Optionen b), c) und d) müssen dem angezeigten Typ entsprechen, der für die Zuweisung erforderlich ist.

Wenn eine Zuweisung mit einem Satz (z. B. Subjekte) zu vervollständigen ist, darf ein Satz an Subjekten aufgelistet werden, aber auch eine kurze Beschreibung des Satzes, aus dem die Elemente von diesem Satz abgeleitet werden können, beispielsweise

- alle Subjekte,
- alle Subjekte vom Typ X,
- alle Subjekte außer Subjekt a oder
- so lange klar ist, welche Subjekte gemeint sind.

7.1.3 Die Operation Auswahl

Eine Auswahloperation tritt auf, wenn eine Komponente ein Element enthält, für das der PP-/ST-Autor aus mehreren Punkten wählen muss.

Wenn ein Element in einem PP eine Auswahl enthält, darf der PP-Autor eine von drei Aufgaben ausführen:

- a) die Auswahl unvollständig lassen;
- b) die Auswahl mit einem oder mehreren Punkten vervollständigen;
- c) die Auswahl durch Entfernen von Optionen einschränken, dabei aber zwei oder mehr aktiv lassen.

Wenn ein Element in einer ST eine Auswahl enthält, muss ein ST-Autor die Auswahl wie oben in b) vervollständigen. Optionen a) und c) sind für STs nicht erlaubt.

Das/die in b) und c) gewählte(n) Punkt(e) müssen Punkte aus der vorgegebenen Auswahl sein.

7.1.4 Die Operation Präzisierung

Die Operation Präzisierung kann für jede Komponente ausgeführt werden. Der PP-/ST-Autor führt eine Präzisierung über eine Änderung der Anforderung durch. Die erste Regel für eine Präzisierung ist, dass ein TOE, der die präzierte Anforderung erfüllt, auch die unpräzierte Anforderung im Kontext des PPs/der ST erfüllt (d. h. eine präzierte Anforderung muss „strenger“ sein, als die ursprüngliche Anforderung). Wenn die Präzisierung diese Regel nicht erfüllt, wird die daraus entstehende Anforderung als eine erweiterte Anforderung betrachtet und muss auch als solche behandelt werden.

Die einzige Ausnahme zu dieser Regel ist, dass es einem PP-/ST-Autor erlaubt ist, eine SFR zu präzisieren, um sie auf einige, aber nicht alle Subjekte, Objekte, Operationen, Sicherheitsattribute und/oder externe Entitäten anzuwenden.

Für zu präzisierende SFRs, die von PPs übernommen werden, mit denen Konformität beansprucht wird, gilt diese Ausnahme allerdings nicht; diese SFRs dürfen nicht präzisiert werden, um weniger Subjekte, Objekte, Operationen, Sicherheitsattribute und/oder externe Entitäten als die SFR im PP anzuwenden.

Die zweite Regel für eine Präzisierung ist, dass die Präzisierung einen Bezug zur ursprünglichen Komponente haben muss.

Ein Sonderfall der Präzisierung ist eine redaktionelle Präzisierung, bei der eine kleine Änderung in der Anforderung durchgeführt wird, d. h. Umformulieren eines Satzes, um der deutschen Grammatik zu entsprechen oder um den Satz verständlicher für die Leser zu gestalten. Eine Bedeutungsänderung der Anforderung ist durch diese Änderung in keinem Fall erlaubt.

7.2 Abhängigkeiten zwischen Komponenten

Zwischen den Komponenten können Abhängigkeiten bestehen. Wenn eine Komponente für sich genommen nicht angemessen ist und auf das Vorhandensein einer anderen Komponente angewiesen ist, um Sicherheitsfunktionalität oder Vertrauenswürdigkeit herzustellen, entstehen Abhängigkeiten.

Die Funktionskomponenten in der ISO/IEC 15408-2 haben üblicherweise Abhängigkeiten zu anderen Funktionskomponenten, und auch einige der Vertrauenswürdigkeitskomponenten in der ISO/IEC 15408-3 haben Abhängigkeiten zu anderen Komponenten in der ISO/IEC 15408-3. Es können auch Abhängigkeiten zwischen Komponenten der ISO/IEC 15408-2 zu Komponenten der ISO/IEC 15408-3 definiert sein. Das hindert allerdings erweiterte Funktionskomponenten nicht daran, Abhängigkeiten zu Vertrauenswürdigkeitskomponenten zu haben oder umgekehrt.

Beschreibungen zu den Abhängigkeiten der Komponenten sind über die Komponentendefinitionen in der ISO/IEC 15408-2 und der ISO/IEC 15408-3 festgelegt. Um die Vollständigkeit der TOE-Sicherheitsanforderungen sicherzustellen, sollten Abhängigkeiten erfüllt sein, wenn Anforderungen, die auf abhängigkeitsbetroffenen Komponenten basieren, in PPs und STs aufgenommen werden. Abhängigkeiten sollten auch bei der Erstellung von Paketen berücksichtigt werden.

Anders ausgedrückt: wenn Komponente A eine Abhängigkeit zu Komponente B hat, folgt daraus, dass für jede auf Komponente A basierende Sicherheitsanforderung eines PPs/einer ST, das PP/die ST auch einen der folgenden Punkte enthalten muss:

- a) eine Sicherheitsanforderung basierend auf Komponente B; oder
- b) eine Sicherheitsanforderung basierend auf einer Komponente, die in der Hierarchie höher liegt als B; oder
- c) eine Begründung, warum das PP/die ST keine Sicherheitsanforderung basierend auf Komponente B enthält.

Wenn eine Sicherheitsanforderung wegen einer Abhängigkeit aufgenommen wird, wie in den Fällen a) und b), kann es erforderlich sein, Operationen (Zuweisung, Iteration, Präzisierung, Auswahl) für diese Sicherheitsanforderung in einer speziellen Weise zu vervollständigen, um sicherzustellen, dass die Abhängigkeit auch wirklich erfüllt wird.

Für den Fall c) sollte die Begründung, dass die Sicherheitsanforderung nicht aufgenommen wird, einen der folgenden Punkte behandeln:

- warum die Abhängigkeit nicht erforderlich oder sinnvoll ist; oder
- dass die Abhängigkeit über die Betriebsumgebung des TOEs behandelt wurde; in diesem Fall sollte in der Begründung beschrieben sein, wie die Sicherheitszielsetzungen für die Betriebsumgebung diese Abhängigkeit behandeln; oder
- dass die Abhängigkeit in irgendeiner anderen Art über andere SFRs behandelt wurde (erweiterte SFRs, Kombinationen von SFRs usw.)

7.3 Erweiterte Komponenten

In der ISO/IEC 15408 ist es verpflichtend, die Anforderungen auf Komponenten aus der ISO/IEC 15408-2 oder der ISO/IEC 15408-3 zu basieren; dabei gelten zwei Ausnahmen:

- a) es gibt Sicherheitszielsetzungen für den TOE, die nicht in SFRs nach Teil 2 übertragen werden können, oder es gibt Anforderungen von Dritten (z. B. Gesetze, Normen), die nicht in SARs nach Teil 3 übertragen werden können (z. B. hinsichtlich Evaluierung von Kryptographie);

- b) eine Sicherheitszielsetzung kann übertragen werden, aber nur mit großen Schwierigkeiten und/oder Komplexität basierend auf Komponenten in der ISO/IEC 15408-2 und/oder ISO/IEC 15408-3.

In beiden Fällen ist es erforderlich, dass der PP-/ST-Autor seine eigenen Komponenten definiert. Diese neu definierten Komponenten werden erweiterte Komponenten genannt. Eine präzise definierte erweiterte Komponente erfordert Kontext und Aussagekraft in Bezug auf die erweiterten SFRs und SARs, die auf diesen Komponenten basieren.

Nachdem die neuen Komponenten korrekt definiert wurden, kann der PP-/ST-Autor anschließend eine oder mehrere SFRs oder SARs auf diese neu definierten erweiterten Komponenten basieren und sie dann genau wie die anderen SFRs und SARs verwenden. Ab diesem Zeitpunkt gibt es keine weitere Unterscheidung mehr zwischen auf der ISO/IEC 15408 basierenden SARs und SFRs und auf erweiterten Komponenten basierenden SARs und SFRs. Siehe ISO/IEC 15408-3 „Extended components definition“ (APE_ECD) und „Extended components definition“ (ASE_ECD) für weitere Anforderungen zu erweiterten Komponenten.

8 Schutzprofile und Pakete

8.1 Einleitung

Um Verbrauchergruppen und Interessengemeinschaften die Darlegung ihrer Sicherheitsbedürfnisse zu ermöglichen, und um das Verfassen von STs zu erleichtern, bietet dieser Teil der ISO/IEC 15408 zwei besondere Konstrukte: Pakete und Schutzprofile (PPs). Die beiden folgenden Unterabschnitte beschreiben diese Konstrukte ausführlicher; anschließend folgt ein Unterabschnitt zur Verwendung dieser Konstrukte.

8.2 Pakete

Ein Paket ist ein benannter Satz an Sicherheitsanforderungen. Ein Paket ist entweder

- ein Funktionspaket, das nur SFRs enthält, oder
- ein Sicherheitspaket, das nur SARs enthält.

Gemischte Pakete, die sowohl SFRs als auch SARs enthalten, sind nicht erlaubt.

Jede Partei kann ein Paket definieren und das Paket ist auf Wiederverwendbarkeit ausgelegt. Für dieses Ziel sollte das Paket nur Anforderungen enthalten, die sowohl sinnvoll als auch effektiv sind. Pakete können beim Aufbau größerer Pakete, PPs und STs verwendet werden. Derzeit gibt es keine Kriterien für die Evaluierung von Paketen, daher kann jeder Satz an SFRs oder SARs ein Paket sein.

Beispiele für Sicherheitspakete sind die in der ISO/IEC 15408-3 definierten Vertrauenswürdigkeitsstufen (EAL-Stufen). Zum Erstellungszeitpunkt gab es keine Funktionspakete für diese Version der ISO/IEC 15408.

8.3 Schutzprofile

Während eine ST stets einen spezifischen TOE beschreibt (z. B. die MinuteGap v18.5 Firewall), ist ein PP für die Beschreibung eines TOE-Typs ausgelegt (z. B. Firewalls). Dasselbe PP kann daher als Vorlage für eine Vielzahl verschiedener STs in verschiedenen Evaluierungen verwendet werden. Eine ausführliche Beschreibung der PPs ist in Anhang B enthalten.

Allgemein beschreibt eine ST Anforderungen an einen TOE und wird vom Entwickler dieses TOEs geschrieben, wohingegen ein PP allgemeine Anforderungen an einen TOE-Typ beschreibt und daher üblicherweise geschrieben wird von

- einer Benutzergruppe, die einen Konsens für die Anforderungen an einen bestimmten TOE-Typ erreichen möchte,

- einem Entwickler eines TOEs, oder einer Gruppe von Entwicklern ähnlicher TOEs, die Mindestanforderungen für diesen TOE-Typ festlegen möchte,
- einer Regierung oder einem großen Unternehmen bei der Festlegung ihrer/seiner Anforderungen als Teil ihres/seines Beschaffungsprozesses.

Das PP bestimmt den erlaubten Konformitätstyp der ST gegenüber dem PP. Das heißt, das PP sagt aus (in der PP-Konformitätserklärung, siehe B.5), welches die erlaubten Konformitätstypen für die ST sind:

- wenn das PP aussagt, dass strikte Konformität erforderlich ist, muss die ST strikt mit dem PP übereinstimmen;
- wenn das PP aussagt, dass nachweisliche Konformität erforderlich ist, muss die ST strikt oder nachweislich mit dem PP übereinstimmen.

Anders ausgedrückt ist eine ST nur für die nachweisliche Konformität in einem PP erlaubt, wenn das PP dies explizit erlaubt.

Wenn eine ST Konformität mit mehreren PPs beansprucht, muss sie (wie oben beschrieben) mit jedem PP wie im entsprechenden PP festgelegt übereinstimmen. Das kann bedeuten, dass die ST mit einigen PPs strikte Konformität erreicht und mit anderen nachweisliche Konformität.

Es ist zu beachten, dass die ST mit dem betreffenden PP entweder konform ist oder nicht. Die ISO/IEC 15408 kennt keine „teilweise“ Konformität. Es liegt daher in der Verantwortung des PP-Autors, dass die PP nicht übermäßig beschwerlich ist und somit PP-/ST-Autoren die Möglichkeit verwehrt, Konformität mit dem PP zu beanspruchen.

Eine ST ist gleichwertig oder restriktiver als ein PP, wenn

- alle die ST erfüllende TOEs auch das PP erfüllen und
- alle das PP erfüllende Betriebsumgebungen auch die ST erfüllen,

oder, informal ausgedrückt, die ST muss die gleichen oder mehr Restriktionen zu diesem TOE aufweisen und die gleichen oder weniger Restriktionen zur Betriebsumgebung des TOEs.

Diese allgemeine Aussage kann für die verschiedenen Unterabschnitte der ST präziser ausgestaltet werden.

a) **Sicherheitsproblemdefinition:** Die Konformitätsbegründung in der ST muss nachweisen, dass die Sicherheitsproblemdefinition in der ST gleichwertig (oder restriktiver) als die Sicherheitsproblemdefinition im PP ist. Das bedeutet, dass

- alle die Sicherheitsproblemdefinition in der ST erfüllenden TOEs auch die Sicherheitsproblemdefinition im PP erfüllen und
- alle die Sicherheitsproblemdefinition in der PP erfüllenden Betriebsumgebungen auch die Sicherheitsproblemdefinition in der ST erfüllen.

b) **Sicherheitszielsetzungen:** Die Konformitätsbegründung in der ST muss nachweisen, dass die Sicherheitszielsetzungen in der ST gleichwertig (oder restriktiver) als die Sicherheitszielsetzungen im PP sind. Das bedeutet, dass

- alle die Sicherheitszielsetzungen in der ST erfüllenden TOEs auch die Sicherheitszielsetzungen für diesen TOE im PP erfüllen und
- alle die Sicherheitszielsetzungen für die Betriebsumgebung in der PP erfüllenden Betriebsumgebungen auch die Sicherheitszielsetzungen für die Betriebsumgebung in der ST erfüllen.