DIN EN ISO/IEC 15408-1

DIN

ICS 35.030

Entwurf

Einsprüche bis 2024-01-24
Vorgesehen als Ersatz für
DIN EN ISO/IEC
15408-1:2020-12

Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre – Evaluationskriterien für IT-Sicherheit – Teil 1: Einführung und allgemeines Modell (ISO/IEC 15408-1:2022); Deutsche und Englische Fassung prEN ISO/IEC 15408-1:2023

Information security, cybersecurity and privacy protection –
Evaluation criteria for IT security –
Part 1: Introduction and general model (ISO/IEC 15408-1:2022);
German and English version prEN ISO/IEC 15408-1:2023

Sécurité de l'information, cybersécurité et protection de la vie privée –
Critères d'évaluation pour la sécurité des technologies de l'information –
Partie 1: Introduction et modèle général (ISO/IEC 15408-1:2022);
Version allemande et anglaise prEN ISO/IEC 15408-1:2023

Anwendungswarnvermerk

Dieser Entwurf mit Erscheinungsdatum 2023-11-24 wird der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt.

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

Stellungnahmen werden erbeten

— vorzugsweise online im Norm-Entwurfs-Portal von DIN unter www.din.de/go/entwuerfe bzw. für Norm-Entwürfe der DKE auch im Norm-Entwurfs-Portal der DKE unter www.entwuerfe.normenbibliothek.de, sofern dort wiedergegeben;

— oder als Datei per E-Mail an nia@din.de möglichst in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter www.din.de/go/stellungnahmen-norm-entwuerfe oder für Stellungnahmen zu Norm-Entwürfen der DKE unter www.dke.de/stellungnahme abgerufen werden;

— oder in Papierform an den DIN-Normenausschuss Informationstechnik und Anwendungen (NIA), 10772 Berlin oder Am DIN-Platz, Burggrafenstr. 6, 10787 Berlin.

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

Gesamtumfang 324 Seiten

DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)

AVA Documents Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-1:2024-01

Nationales Vorwort

Der Text von ISO/IEC 15408-1:2022 wurde vom Technischen Komitee ISO/IEC JTC 1 „Information technology“ der Internationalen Organisation für Normung (ISO) erarbeitet und als prEN ISO/IEC 15408-1:2023 durch das Technische Komitee CEN/CLC/JTC 13 „Cybersicherheit und Datenschutz“ übernommen, dessen Sekretariat von DIN (Deutschland) gehalten wird.

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

Um Zweifelsfälle in der Übersetzung auszuschließen, ist die englische Originalfassung beigefügt. 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 18045	siehe	DIN EN ISO/IEC 18045
ISO/IEC 19790	siehe	DIN EN ISO/IEC 19790
ISO/IEC 19896-1	siehe	DIN EN ISO/IEC 19896-1
ISO/IEC 19896-3	siehe	DIN EN ISO/IEC 19896-3
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 DIN EN ISO/IEC 15408-1:2020-12 wurden folgende Änderungen vorgenommen:

a) Dokument umstrukturiert;

b) technische Änderungen eingeführt;

c) Terminologie überprüft und aktualisiert;

d) genaue Konformitätstyp eingeführt;

e) Schutzprofile (PPs) mit geringer Sicherheit entfernt und PPs mit direkter Begründung eingeführt;

f) PP-Module und PP-Konfigurationen für modulare Evaluierungen eingeführt;

g) Mehrfachsicherungsbewertung eingeführt.

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-1:2024-01

Nationaler Anhang NA
(informativ)

Literaturhinweise

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

DIN EN ISO/IEC 19790, *Informationstechnik — Sicherheitstechniken — Sicherheitsanforderungen für kryptografische Module*

DIN EN ISO/IEC 19896-1, *IT-Sicherheitstechniken — Kompetenzanforderungen an Tester und Evaluatoren von Informationssicherheit — Teil 1: Einführung, Konzepte und allgemeine Anforderungen*

DIN EN ISO/IEC 19896-3, *IT-Sicherheitstechniken — Kompetenzanforderungen an Tester und Evaluatoren von Informationssicherheit — Teil 3: Anforderungen an die Kenntnisse, Fähigkeiten und Effektivität von Evaluatoren nach ISO/IEC 15408*

DIN EN ISO/IEC 27001, *Informationssicherheit, Cybersicherheit und Datenschutz — Informationssicherheitsmanagementsysteme — Anforderungen*

DIN EN ISO/IEC 27002, *Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre — Informationssicherheitsmaßnahmen*

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-1:2024-01

– Leerseite –

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-1:2024-01

– Entwurf –

Juli 2023

prEN ISO/IEC 15408-1

Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre – Evaluationskriterien für IT-Sicherheit – Teil 1: Einführung und allgemeines Modell (ISO/IEC 15408-1:2022)

Information security, cybersecurity and privacy protection – Evaluation criteria for IT security – Part 1: Introduction and general model (ISO/IEC 15408-1:2022)

Sécurité de l'information, cybersécurité et protection de la vie privée – Critères d'évaluation pour la sécurité des technologies de l'information – Partie 1: Introduction et modèle général (ISO/IEC 15408-1:2022)

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-1:2024-01

Inhalt

Seite

Europäisches Vorwort . . . 7
Vorwort . . . 8
Einleitung . . . 11
1 Anwendungsbereich . . . 13
2 Normative Verweisungen . . . 13
3 Begriffe . . . 13
4 Symbole und Abkürzungen . . . 26
5 Übersicht . . . 28
5.1 Allgemein . . . 28
5.2 Beschreibung der Normenreihe ISO/IEC 15408 . . . 28
5.2.1 Allgemein . . . 28
5.2.2 Zielgruppe . . . 29
5.3 Evaluierungsgegenstand (TOE) . . . 33
5.3.1 Allgemein . . . 33
5.3.2 TOE-Grenzen . . . 33
5.3.3 Unterschiedliche Darstellungen des TOEs . . . 34
5.3.4 Unterschiedliche Konfigurationen des TOEs . . . 34
5.3.5 Betriebsumgebung des TOE . . . 35
5.4 Darstellung des Inhalts dieses Dokuments . . . 35
6 Allgemeines Modell . . . 35
6.1 Hintergrund . . . 35
6.2 Vermögenswerte und Sicherheitsmaßnahmen . . . 36
6.3 Kernkonstrukte des Paradigmas der Normenreihe ISO/IEC 15408 . . . 38
6.3.1 Allgemein . . . 38
6.3.2 Konformitätstypen . . . 39
6.3.3 Weitergabe von Sicherheitsanforderungen . . . 39
6.3.4 Erfüllung der Bedürfnisse der Verbraucher (Risikoeigentümer) . . . 42
7 Festlegung von Sicherheitsanforderungen . . . 44
7.1 Sicherheitsproblemdefinition (SPD) . . . 44
7.1.1 Allgemein . . . 44
7.1.2 Bedrohungen . . . 44
7.1.3 Organisatorische Sicherheitsrichtlinien (OSP) . . . 45
7.1.4 Annahmen . . . 45
7.2 Sicherheitszielsetzungen . . . 46
7.2.1 Allgemein . . . 46
7.2.2 Sicherheitszielsetzungen für den TOE . . . 47
7.2.3 Sicherheitszielsetzungen für die Betriebsumgebung . . . 47
7.2.4 Beziehung zwischen Sicherheitszielsetzungen und der SPD . . . 47
7.2.5 Rückverfolgung zwischen Sicherheitszielsetzungen und der SPD . . . 48
7.2.6 Bereitstellen einer Begründung für die Rückverfolgung . . . 48
7.2.7 Zum Entgegenwirken von Bedrohungen . . . 49
7.2.8 Sicherheitszielsetzungen: Schlussfolgerung . . . 49
7.3 Sicherheitsanforderungen . . . 50
7.3.1 Allgemein . . . 50
7.3.2 Sicherheitsfunktionsanforderungen (SFR) . . . 50
7.3.3 Vertrauenswürdigkeitsanforderungen (SARs) . . . 52
7.3.4 Sicherheitsanforderungen: Schlussfolgerung . . . 53
8 Sicherheitskomponenten . . . 55
8.1 Hierarchische Struktur der Sicherheitskomponenten . . . 55
8.1.1 Allgemein . . . 55
8.1.2 Klasse . . . 55

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-1:2024-01

8.1.3 Familie . . . 55
8.1.4 Komponente . . . 55
8.1.5 Element . . . 55
8.2 Operationen . . . 56
8.2.1 Allgemein . . . 56
8.2.2 Iteration . . . 56
8.2.3 Zuweisung . . . 57
8.2.4 Auswahl . . . 58
8.2.5 Präzisierung . . . 59
8.3 Abhängigkeiten zwischen Komponenten . . . 61
8.4 Erweiterte Komponenten . . . 61
8.4.1 Allgemein . . . 61
8.4.2 Definieren erweiterter Komponenten . . . 62
9 Pakete . . . 63
9.1 Allgemein . . . 63
9.2 Pakettypen . . . 63
9.2.1 Allgemein . . . 63
9.2.2 Vertrauenswürdigkeitspakete . . . 64
9.2.3 Funktionspakete . . . 64
9.3 Paketabhängigkeiten . . . 65
9.4 Evaluierungsmethode(n) und -aufgaben . . . 65
10 Schutzprofile (PP) . . . 65
10.1 Allgemein . . . 65
10.2 PP-Einleitung . . . 65
10.3 Konformitätsansprüche und Konformitätserklärungen . . . 66
10.4 Vertrauenswürdigkeitsanforderungen (SARs) . . . 69
10.5 Zusätzliche gemeinsame Anforderungen an die strikte und nachweisliche Konformität . . . 69
10.5.1 Konformitätsansprüche und Konformitätserklärungen . . . 69
10.5.2 Sicherheitsproblemdefinition (SPD) . . . 69
10.5.3 Sicherheitszielsetzungen . . . 69
10.6 Zusätzliche Anforderungen speziell für die strikte Konformität . . . 70
10.6.1 Anforderungen an die Sicherheitsproblemdefinition (SPD) . . . 70
10.6.2 Anforderungen an die Sicherheitszielsetzungen . . . 70
10.6.3 Anforderungen an die Sicherheitsanforderungen . . . 70
10.7 Zusätzliche Anforderungen speziell für die nachweisliche Konformität . . . 71
10.8 Zusätzliche Anforderungen speziell für die genaue Konformität . . . 71
10.8.1 Allgemein . . . 71
10.8.2 Konformitätsansprüche und -erklärungen . . . 71
10.9 Unter Verwendung von PP . . . 72
10.10 Konformitätserklärungen und -ansprüche im Falle mehrerer PP . . . 72
10.10.1 Allgemein . . . 72
10.10.2 Wenn strikte oder nachweisliche Konformität festgelegt ist . . . 72
10.10.3 Wenn genaue Konformität festgelegt ist . . . 72
11 Modularer Aufbau der Anforderungen . . . 73
11.1 Allgemein . . . 73
11.2 PP-Module . . . 73
11.2.1 Allgemein . . . 73
11.2.2 PP-Modulbasis . . . 73
11.2.3 Anforderungen an PP-Module . . . 73
11.3 PP-Konfigurationen . . . 77
11.3.1 Allgemein . . . 77
11.3.2 Anforderungen an PP-Konfigurationen . . . 78
11.3.3 Verwendung von PP-Konfigurationen . . . 84
12 Sicherheitsvorgaben (ST) . . . 87
12.1 Allgemein . . . 87
12.2 Konformitätsansprüche und -erklärungen . . . 88
12.3 Vertrauenswürdigkeitsanforderungen . . . 90

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-1:2024-01

12.4 Zusätzliche Anforderungen im Fall der genauen Konformität . . . 91
12.4.1 Zusätzliche Anforderungen für den Konformitätsanspruch . . . 91
12.4.2 Zusätzliche Anforderungen für die SPD . . . 91
12.4.3 Zusätzliche Anforderungen an die Sicherheitszielsetzungen . . . 91
12.4.4 Zusätzliche Anforderungen an die Sicherheitsanforderungen . . . 92
12.5 Zusätzliche Anforderungen im Fall der Mehrfach-Vertrauenswürdigkeit . . . 92
13 Evaluierung und Evaluierungsergebnisse . . . 94
13.1 Allgemein . . . 94
13.2 Evaluierungskontext . . . 96
13.3 Evaluierung der PP und PP-Konfigurationen . . . 97
13.4 Evaluierung von ST . . . 98
13.5 Evaluierung von TOE . . . 98
13.6 Evaluierungsmethoden und Evaluierungsaufgaben . . . 98
13.7 Evaluierungsergebnisse . . . 99
13.7.1 Ergebnisse einer PP-Evaluierung . . . 99
13.7.2 Ergebnisse der Evaluierung einer PP-Konfiguration . . . 99
13.7.3 Ergebnisse einer ST-/TOE-Evaluierung . . . 99
13.8 Evaluierung mit Mehrfach-Vertrauenswürdigkeit . . . 100
14 Zusammensetzung der Vertrauenswürdigkeit . . . 101
14.1 Allgemein . . . 101
14.2 Zusammensetzungsmodelle . . . 102
14.2.1 Mehrschichtiges Zusammensetzungsmodell . . . 102
14.2.2 Netzwerk- oder bi-direktionales Zusammensetzungsmodell . . . 103
14.2.3 Eingebettetes Zusammensetzungsmodell . . . 103
14.3 Evaluierungstechniken für die Vertrauenswürdigkeit von Zusammensetzungsmodellen . 104
14.3.1 Allgemein . . . 104
14.3.2 ACO-Klasse für zusammengesetzte TOE . . . 104
14.3.3 Verbundevaluation für Verbundprodukte . . . 105
14.4 Anforderungen an Evaluierungen, die Zusammensetzungstechniken verwenden . . . 117
14.4.1 Wiederverwendung von Evaluierungsergebnissen . . . 117
14.4.2 Aspekte der zusammengesetzten Evaluierung . . . 118
14.5 Evaluierung mittels Zusammensetzung und Mehrfach-Vertrauenswürdigkeit . . . 119
Anhang A (normativ) Spezifikation von Paketen . . . 121
A.1 Ziel und Aufbau dieses Anhangs . . . 121
A.2 Paketfamilien . . . 121
A.2.1 Allgemein . . . 121
A.2.2 Name der Paketfamilie . . . 121
A.2.3 Überblick über die Paketfamilie . . . 121
A.2.4 Zielsetzungen der Paketfamilie . . . 121
A.2.5 Pakete . . . 121
A.3 Pakete . . . 121
A.3.1 Verpflichtender Inhalt eines Pakets . . . 121
A.3.2 Optionaler Inhalt eines Pakets . . . 123
Anhang B (normativ) Spezifikation von Schutzprofilen (PP) . . . 125
B.1 Ziel und Aufbau dieses Anhangs . . . 125
B.2 Spezifikation eines PP . . . 125
B.2.1 Wie ein PP verwendet werden sollte . . . 125
B.2.2 Wie ein PP nicht verwendet werden sollte . . . 126
B.3 Verpflichtender Inhalt eines PPs . . . 126
B.3.1 Allgemein . . . 126
B.3.2 PP-Einleitung (APE_INT) . . . 128
B.3.3 Konformitätsansprüche und Konformitätserklärung (APE_CCL) . . . 130
B.3.4 Sicherheitsproblemdefinition (SPD) (APE_SPD) . . . 131
B.3.5 Sicherheitszielsetzungen (APE_OBJ) . . . 131
B.3.6 Erweiterte Komponentendefinition (APE_ECD) . . . 131
B.3.7 Sicherheitsanforderungen (APE_REQ) . . . 131
B.4 Verweisen auf andere Normen in einem PP . . . 132

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-1:2024-01

B.5 Die PP mit direkter Begründung . . . 133
B.5.1 Allgemein . . . 133
B.5.2 Konformitätsansprüche (APE_CCL) für die PP mit direkter Begründung . . . 134
B.5.3 Sicherheitszielsetzungen (APE_OBJ) für PP mit direkter Begründung . . . 134
B.6 Optionaler Inhalt eines PP . . . 135
Anhang C (normativ) Spezifikation von PP-Modulen und PP-Konfigurationen . . . 136
C.1 Ziel und Aufbau dieses Anhangs . . . 136
C.2 Spezifikation von PP-Modulen . . . 136
C.2.1 Unter Verwendung eines PP-Moduls . . . 136
C.2.2 Verpflichtender Inhalt eines PP-Moduls . . . 136
C.2.3 PP-Module mit direkter Begründung . . . 143
C.2.4 Leitlinien für die Einbeziehung von SPD-Elementen aus einer PP-Modulbasis . . . 143
C.2.5 Optionaler Inhalt eines PP-Moduls . . . 144
C.3 Spezifikation von PP-Konfigurationen . . . 144
C.3.1 Allgemein . . . 144
C.3.2 PP-Konfigurationsverweisung . . . 146
C.3.3 Komponentenerklärung . . . 146
C.3.4 TOE-Überblick . . . 146
C.3.5 Konsistenzbegründung . . . 146
C.3.6 Konformitätsanspruch und Konformitätserklärung . . . 146
C.3.7 SAR-Aussage . . . 149
Anhang D (normativ) Spezifikation von Sicherheitsvorgaben (ST) und ST mit direkter Begründung . . . 150
D.1 Ziel und Aufbau dieses Anhangs . . . 150
D.2 Verwendung einer ST . . . 150
D.2.1 Wie eine ST verwendet werden sollte . . . 150
D.2.2 Wie eine ST nicht verwendet werden sollte . . . 151
D.2.3 Fragen, die mit einer ST beantwortet werden können . . . 151
D.3 Verpflichtender Inhalt einer ST . . . 152
D.3.1 Allgemein . . . 152
D.3.2 ST-Einleitung (ASE_INT) . . . 154
D.3.3 Konformitätsansprüche (ASE_CCL) . . . 157
D.3.4 Sicherheitsproblemdefinition (SPD) (ASE_SPD) . . . 157
D.3.5 Sicherheitszielsetzungen (ASE_OBJ) . . . 157
D.3.6 Erweiterte Komponentendefinition (ASE_ECD) . . . 157
D.3.7 Sicherheitsanforderungen (ASE_REQ) . . . 157
D.3.8 Zusammenfassende Spezifikation des TOEs (ASE_TSS) . . . 159
D.4 ST mit direkter Begründung . . . 159
D.4.1 Allgemein . . . 159
D.4.2 Konformitätsansprüche (ASE_CCL) für ST mit direkter Begründung . . . 161
D.4.3 Sicherheitsproblemdefinition (SPD) (ASE_SPD) für ST mit direkter Begründung . . . 161
D.4.4 Sicherheitsanforderungen (ASE_REQ) für ST mit direkter Begründung. . . . 161
D.5 Verweisen auf andere Normen in einer ST . . . 161
Anhang E (normativ) Konformität des/der PP/PP-Konfiguration . . . 162
E.1 Allgemein . . . 162
E.2 Nachweisliche Konformität . . . 163
E.3 Strikte Konformität . . . 163
E.4 Genaue Konformität . . . 163
E.4.1 Allgemein . . . 163
E.4.2 FAQ/Cheatsheet zu genauer Konformität . . . 166
Literaturhinweise . . . 168

Bilder

Bild 1 — Sicherheitskonzepte und Beziehungen . . . 37

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-1:2024-01

Bild 2 — Evaluierungskonzepte und Beziehungen 38
Bild 3 — Rückverfolgungen zwischen Sicherheitszielsetzungen und der SPD 48
Bild 4 — Beziehungen zwischen SPD, Sicherheitszielsetzungen und Sicherheitsanforderungen . 54
Bild 5 — Beispiel einer PP-Konfiguration 84
Bild 6 — Verwendung von PP-Konfigurationen mit Einfach- und Mehrfach-Vertrauenswürdigkeit 85
Bild 7 — Zusammensetzung von PP-Komponenten 86
Bild 8 — Vertrauenswürdigkeitsklassen, die zur Evaluierung der PP, PP-Konfigurationen und ST verwendet werden 87
Bild 9 — Beispiel einer ST mit Mehrfach-Vertrauenswürdigkeit 94
Bild 10 — Ablauf der Evaluierung 95
Bild 11 — Mehrschichtiges Zusammensetzungsmodell 102
Bild 12 — Netzwerk- oder bi-direktionales Zusammensetzungsmodell 103
Bild 13 — Eingebettetes Zusammensetzungsmodell 104
Bild 14 — Unter Verwendung der ACO-Klasse evaluierter zusammengesetzter TOE 105
Bild 15 — Verbundevaluation 107
Bild A.1 — Aufbau einer Paketfamilie mit Vertrauenswürdigkeits- oder Funktionspaketen 122
Bild B.1 — Inhalt eines Schutzprofils 127
Bild B.2 — Inhalt eines PP mit direkter Begründung 134
Bild C.1 — Inhalt eines PP-Moduls 137
Bild C.2 — Übernommene Konformitätsansprüche und -erklärungen für den Fall der genauen Konformität 140
Bild C.3 — Inhalte eines PP-Moduls mit direkter Begründung 143
Bild C.4 — Inhalt einer PP-Konfiguration 145
Bild C.5 — PP-Konfiguration und genaue Konformität 148
Bild D.1 — Inhalt einer ST 153
Bild D.2 — Inhalt einer ST mit direkter Begründung 160
Bild E.1 — Genaue Konformität einer ST mit mehreren PP 164
Bild E.2 — Genaue Konformität mit einer PP-Konfiguration mit mehreren PP und PP-Modulen . 166

Tabellen

Tabelle 1 — Roadmap für die „Evaluierungskriterien für IT-Sicherheit“ 31
Tabelle 2 — Informationen, die dem Entwickler der abhängigen Komponente zur Verfügung zu stellen sind 109
Tabelle 3 — Informationen, die dem Evaluator für Verbundprodukte und der Evaluierungsinstanz für Verbundprodukte zur Verfügung zu stellen sind 110
Tabelle E.1 — Zusammenfassung der genauen Konformität 166

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-1:2024-01

Europäisches Vorwort

Der Text von ISO/IEC 15408-1:2022 wurde vom Technischen Komitee ISO/IEC JTC 1 „Information technology“ der Internationalen Organisation für Normung (ISO) erarbeitet und vom Technischen Komitee CEN/CLC/JTC 13 „Cybersicherheit und Datenschutz“ als prEN ISO/IEC 15408-1:2023 übernommen, dessen Sekretariat von DIN gehalten wird.

Dieses Dokument ist derzeit zur CEN-Umfrage vorgelegt.

Dieses Dokument wird EN ISO/IEC 15408-1:2020 ersetzen.

Rückmeldungen oder Fragen zu diesem Dokument sollten an das jeweilige nationale Normungsinstitut des Anwenders gerichtet werden. Eine vollständige Liste dieser Institute ist auf den Internetseiten von CEN abrufbar.

Anerkennungsnotiz

Der Text von ISO/IEC 15408-1:2022 wurde von CEN als prEN ISO/IEC 15408-1:2023 ohne irgendeine Abänderung genehmigt.

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-1:2024-01

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. Weitere internationale staatliche und nichtstaatliche Organisationen, die in engem Kontakt mit ISO und IEC stehen, nehmen ebenfalls an der Arbeit teil.

Die Verfahren, die bei der Entwicklung dieses Dokuments angewendet wurden und die für die weitere Pflege vorgesehen sind, werden in den ISO/IEC-Directives, Teil 1 beschrieben. Im Besonderen sollten die für die verschiedenen ISO-Dokumentenarten notwendigen Annahmekriterien beachtet werden. Dieses Dokument wurde in Übereinstimmung mit den Gestaltungsregeln der ISO/IEC-Directives, Teil 2 erarbeitet (siehe www.iso.org/directives oder www.iec.ch/members_experts/refdocs).

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. ISO und IEC sind nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren. Details zu allen während der Entwicklung des Dokuments identifizierten Patentrechten finden sich in der Einleitung und/oder in der ISO-Liste der erhaltenen Patenterklärungen (siehe www.iso.org/patents) oder in der IEC-Liste der erhaltenen Patenterklärungen (siehe http://patents.iec.ch).

Jeder in diesem Dokument verwendete Handelsname dient nur zur Unterrichtung der Anwender und bedeutet keine Anerkennung.

Für eine Erläuterung des freiwilligen Charakters von Normen, der Bedeutung ISO-spezifischer Begriffe und Ausdrücke in Bezug auf Konformitätsbewertungen sowie Informationen darüber, wie ISO die Grundsätze der Welthandelsorganisation (WTO, en: World Trade Organization) hinsichtlich technischer Handelshemmnisse (TBT, en: Technical Barriers to Trade) berücksichtigt, siehe www.iso.org/iso/foreword.html. In der IEC, siehe www.iec.ch/understanding-standards.

Dieses Dokument wurde vom gemeinsamen Technischen Komitee ISO/IEC JTC 1, *Information technology*, Unterkomitee SC 27, *Information security, cybersecurity and privacy protection* erarbeitet.

Diese vierte Ausgabe ersetzt die dritte Ausgabe (ISO/IEC 15408-1:2009), die technisch überarbeitet wurde.

Die wesentlichen Änderungen sind folgende:

— das Dokument wurde neu strukturiert;

— technische Änderungen wurden eingeführt:

  — die Terminologie wurde überprüft und aktualisiert;

  — der genaue Konformitätstyp wurde eingeführt;

  — die Schutzprofile (PP) mit niedriger Vertrauenswürdigkeit wurden entfernt und die PP mit direkter Begründung eingeführt;

  — PP-Module und PP-Konfigurationen für modulare Evaluierungen wurden eingeführt;

  — eine Evaluierung mit Mehrfach-Vertrauenswürdigkeit wurde eingeführt.

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-1:2024-01

Eine Auflistung aller Teile der Normenreihe ISO/IEC15408 ist auf der ISO- und auf der IEC-Internetseite abrufbar.

Rückmeldungen oder Fragen zu diesem Dokument sollten an das jeweilige nationale Normungsinstitut des Anwenders gerichtet werden. Eine vollständige Auflistung dieser Institute ist unter www.iso.org/members.html und www.iec.ch/national-committees zu finden.

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-1:2024-01

Rechtliche Hinweise

Die unten aufgeführten Regierungsorganisationen haben zu der Entwicklung dieser Version der „Common Criteria for Information Technology Security Evaluations“ beigetragen. Als gemeinsame Urheberrechtsinhaber an den Common Criteria for Information Technology Security Evaluations (kurz CC) erteilen sie hiermit der ISO/IEC die nicht-exklusive Lizenz zur Verwendung der CC für die weitere Entwicklung/Pflege der Normenreihe ISO/IEC 15408. Diese Regierungsorganisationen behalten sich allerdings das Recht zur Nutzung, Vervielfältigung, zum Vertrieb sowie zur Übersetzung und Änderung der CC nach Belieben vor.

Australien	Australian Signals Directorate
Kanada	Communications Security Establishment
Frankreich	Agence Nationale de la Sécurité des Systèmes d’Information
Deutschland	Bundesamt für Sicherheit in der Informationstechnik
Japan	Information-technology Promotion Agency
Niederlande	Netherlands National Communications Security Agency
Neuseeland	Government Communications Security Bureau
Republik Korea	National Security Research Institute
Spanien	Ministerio de Asuntos Económicos y Transformación Digital
Schweden	FMV, Swedish Defence Materiel Administration
Vereinigtes Königreich	National Cyber Security Centre
USA	National Security Agency

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-1:2024-01

Einleitung

Die Normenreihe ISO/IEC 15408 ermöglicht die Vergleichbarkeit der Ergebnisse unabhängiger Sicherheitsevaluierungen 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 können 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 Normenreihe ISO/IEC 15408 ist hilfreich als Leitfaden für Entwicklung, Evaluierung und/oder Beschaffung von IT-Produkten mit Sicherheitsfunktionalität.

Die Normenreihe ISO/IEC 15408 ist absichtlich flexibel gestaltet, um einen großen Bereich an Evaluierungsansätzen 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 Normenreihe ISO/IEC 15408 beispielsweise in Verbindung mit ungeeigneten Evaluierungsmethoden/-aufgaben, 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. Evaluierungsstellen wird empfohlen, Produkte, Eigenschaften und Methoden zur Bestimmung, ob eine Evaluierung bedeutungsvolle Ergebnisse liefert, 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 nützlich und anwendbar ist.

Die Normenreihe 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 Normenreihe ISO/IEC 15408 kann auch anwendbar sein auf Bereiche der IT-Sicherheit, die über diese drei Kategorien hinausgehen. Die Normenreihe ISO/IEC 15408 ist anwendbar auf von Menschen ausgelöste Risiken (böswillig oder anders geartet) und auf nicht von Menschen ausgelöste Risiken. Die Normenreihe ISO/IEC 15408 darf 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 Normenreihe ISO/IEC 15408, weil sie besondere Techniken umfassen oder nur am Rande Teil der IT-Sicherheit sind. Einige dieser Themen sind unten aufgeführt:

a) die Normenreihe 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) die Normenreihe ISO/IEC 15408 behandelt nicht die Evaluierungsmethodologie, mit der die Kriterien angewendet werden sollten;

   ANMERKUNG 1 Die grundlegende Methodologie ist in ISO/IEC 18045 definiert. ISO/IEC 15408-4 kann zur weiteren Ableitung von Evaluierungsaufgaben und -methoden aus ISO/IEC 18045 verwendet werden.

c) die Normenreihe 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

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-1:2024-01

Normenreihe ISO/IEC 15408 für Evaluierungszwecke im Zusammenhang mit einem solchen Rahmenwerk verwendet werden soll;

d) die Verfahren zur Verwendung von Evaluierungsergebnissen in Akkreditierungen liegen außerhalb des Anwendungsbereichs der Normenreihe 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, müssen Akkreditierer gesonderte Bestimmungen für diese Aspekte treffen;

e) die Kriterien für die Bewertung der charakteristischen Qualitäten von kryptographischen Algorithmen werden nicht in der Normenreihe ISO/IEC 15408 behandelt. Wenn eine unabhängige Bewertung der mathematischen Eigenschaften der Kryptographie erforderlich ist, so muss der in der Normenreihe ISO/IEC 15408 angewendete Evaluierungsplan solch eine Bewertung vorsehen.

ANMERKUNG 2 Im vorliegenden Dokument werden einige Begriffe fett und kursiv gedruckt, um sie vom übrigen Text abzuheben. Die Beziehung zwischen den Komponenten einer Familie wird als Konvention über eine Fettmarkierung hervorgehoben. Diese Markierungskonvention erfordert die Verwendung von Fettdruck für alle neuen Anforderungen. Für hierarchische Komponenten werden Anforderungen fett hervorgehoben, wenn sie über die Anforderungen der vorherigen Komponente hinaus erweitert oder geändert werden. Zusätzlich werden alle neuen oder erweiterten zulässigen über die vorherige Komponente hinausgehenden Operationen auch fett hervorgehoben.

Die Verwendung von Kursivschrift weist auf einen Text hin, der eine genaue Bedeutung hat. Für die Vertrauenswürdigkeitsanforderungen gilt die Konvention für spezielle Verben, die sich auf die Evaluierung beziehen.

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-1:2024-01

1 Anwendungsbereich

Dieses Dokument legt die allgemeinen Konzepte und Prinzipien der IT-Sicherheitsevaluierung fest und bestimmt das allgemeine Evaluierungsmodell, das in verschiedenen Teilen der Norm verwendet wird, und das in seiner Gesamtheit als Grundlage für die Evaluierung der Sicherheitseigenschaften von IT-Produkten vorgesehen ist.

Dieses Dokument bietet einen Überblick über alle Teile der Normenreihe ISO/IEC 15408. Es beschreibt die verschiedenen Teile der Normenreihe ISO/IEC 15408, definiert die Begriffe und Abkürzungen zur Verwendung in allen Teilen der Norm, legt das Kernkonzept des Evaluierungsgegenstands (TOE; en: target of evaluation) fest, beschreibt den Evaluierungszusammenhang und die Zielgruppe, an die sich die Evaluierungskriterien richten. Zu den für die Evaluierung von IT-Produkten erforderlichen, grundlegenden Sicherheitskonzepten wird eine Einführung gegeben.

Dieses Dokument führt in folgende Sachverhalte ein:

— die grundlegenden Konzepte von Schutzprofilen (PP), PP-Modulen, PP-Konfigurationen, Paketen, Sicherheitsvorgaben (ST) und Konformitätstypen;

— eine Beschreibung der Organisation von Sicherheitskomponenten im gesamten Modell;

— 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;

— allgemeine Informationen über die in ISO/IEC 18045 beschriebenen Evaluierungsmethoden;

— Leitlinien für die Anwendung der ISO/IEC 15408-4 zur Entwicklung von Evaluierungsmethoden (EM) und Evaluierungsaufgaben (EA), die aus ISO/IEC 18045 abgeleitet werden;

— allgemeine Informationen über die vordefinierten Vertrauenswürdigkeitsstufen (EAL-Stufen), die in ISO/IEC 15408-5 definiert sind;

— Informationen über den Anwendungsbereich der Evaluierungspläne.

2 Normative Verweisungen

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

ISO/IEC 15408-2:2022, *Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 2: Security functional components*

ISO/IEC 15408-3:2022, *Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 3: Security assurance components*

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

ISO/IEC IEEE 24765, *Systems and software engineering — Vocabulary*

3 Begriffe

Für die Anwendung dieses Dokuments gelten die Begriffe nach ISO/IEC 15408-2, ISO/IEC 15408-3, ISO/IEC 18045 und ISO/IEC IEEE 24765.

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-1:2024-01

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

— ISO Online Browsing Platform: verfügbar unter https://www.iso.org/obp

— IEC Electropedia: verfügbar unter https://www.electropedia.org/

3.1
Aktion
dokumentierte Aufgabe des *Evaluators* (3.45) oder *Entwicklers* (3.33)

Anmerkung 1 zum Begriff: Evaluatorenaktionen und Entwickleraktionen werden durch ISO/IEC 15408-3 gefordert.

3.2
Administrator
Entität (3.36), die bezüglich aller durch die *TOE-Sicherheitsfunktionalität (TSF)* (3.92) implementierten Richtlinien einen Vertrauensgrad besitzt

Anmerkung 1 zum Begriff: Nicht alle *Schutzprofile (PP)* (3.68) oder Sicherheitsvorgaben (ST) nehmen für Administratoren den gleichen Vertrauensgrad an. Üblicherweise wird angenommen, dass Administratoren jederzeit die in der ST des *Evaluierungsgegenstandes (TOE)* (3.90) definierten Richtlinien einhalten. Manche dieser Richtlinien können mit der Funktionalität des TOEs in Zusammenhang stehen, während andere mit der *Betriebsumgebung* (3.63) zusammenhängen.

3.3
nachteilige Aktion
Aktion (3.1), die von einem *Bedrohungsagenten* (3.91) gegen ein *Schutzobjekt* (3.4) durchgeführt wird

3.4
Vermögenswert
Entität (3.36), von der anzunehmen ist, dass sie für den Eigentümer des *Evaluierungsgegenstands (TOE)* (3.90) einen Wert darstellt

3.5
Zuweisung
Spezifikation eines bezeichneten Parameters in einer Funktions- oder Vertrauenswürdigkeitskomponente

3.6
Vertrauenswürdigkeit
Vertrauensgrundlage, dass ein *Evaluierungsgegenstand (TOE)* (3.90) die *Sicherheitsfunktionsanforderungen (SFR)* (3.78) einhält

3.7
Vertrauenswürdigkeitspaket
benannter Satz von *Vertrauenswürdigkeitsanforderungen* (3.76)

BEISPIEL „EAL 3“.

3.8
Angriffspotential
Maß für den Aufwand, der erforderlich ist, um eine Anfälligkeit in einem *Evaluierungsgegenstand (TOE)* (3.90) auszunutzen

Anmerkung 1 zum Begriff: Der Aufwand wird als Funktion der Eigenschaften des Angreifers (z. B. Fachwissen, Ressourcen und Motivation) und der Eigenschaften der Anfälligkeit selbst (z. B. Zugriffsgelegenheit, Zeit bis zur Aufdeckung) ausgedrückt.

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-1:2024-01

3.9
Angriffsfläche
Menge logischer oder physischer Schnittstellen zu einer Zielvorgabe, bestehend aus Punkten, über die versucht wird, auf die Zielvorgabe und ihre Funktionen zuzugreifen.

BEISPIEL 1 Das Gehäuse eines Zahlungsterminals ist ein Teil der physischen Angriffsfläche für dieses Gerät.

BEISPIEL 2 Die Kommunikationsprotokolle, die für die Verbindung mit einem Netzwerkgerät zur Verfügung stehen, sind Teil der logischen Angriffsfläche für dieses Netzwerkgerät.

3.10
Erweiterung
Hinzufügen von einer oder mehreren Anforderungen zu einem Paket

Anmerkung 1 zum Begriff: Im Falle eines *Funktionspakets* (3.51) wird eine solche Erweiterung nur im Zusammenhang mit einem Paket betrachtet und nicht im Zusammenhang mit anderen Paketen oder *Schutzprofilen (PP)* (3.68) bzw. *Sicherheitsvorgaben (ST)* (3.82).

Anmerkung 2 zum Begriff: Im Falle eines *Vertrauenswürdigkeitspakets* (3.7) bezieht sich die Ergänzung auf eine oder mehrere *Vertrauenswürdigkeitsanforderungen (SAR)* (3.76).

3.11
autorisierter Benutzer
Entität (3.36), die in Übereinstimmung mit den *Sicherheitsfunktionsanforderungen (SFR)* (3.78) eine Operation am *Evaluierungsgegenstand (TOE)* (3.90) durchführen darf

3.12
Basiskomponente
unabhängige Entität (3.36) in einem Mehrkomponentenprodukt, die einer oder mehreren *abhängigen Komponente(n)* (3.31) Dienste und Ressourcen zur Verfügung stellt

Anmerkung 1 zum Begriff: Dies gilt insbesondere für „*zusammengesetzte TOE*“ (3.21) und „Verbundprodukte/*Verbund-TOE*“ (3.25).

3.13
Basisschutzprofil
Basis-PP
Schutzprofil (3.68), das in einem PP-Modul (3.71) als Teil der *PP-Modulbasis* (3.72) dieses PP-Moduls festgelegt ist und als Grundlage für die Erstellung einer *PP-Konfiguration* (3.69) dient

3.14
Basis-PP-Modul
PP-Modul (3.71), das in einem anderen PP-Modul als Teil der *PP-Modulbasis* (3.72) dieses PP-Moduls festgelegt ist und als Grundlage für die Erstellung einer *PP-Konfiguration* (3.69) dient

Anmerkung 1 zum Begriff: Die Spezifikation eines Basis-PP-Moduls in einem PP-Modul schließt implizit die PP-Modulbasis des Basis-PP-Moduls ein.

3.15
Basisevaluierungsgegenstand
Basis-TOE
Basiskomponente (3.12), die selbst Gegenstand einer Evaluierung ist

Anmerkung 1 zum Begriff: Dies gilt insbesondere für „*zusammengesetzte TOE*“ (3.21) und „Verbundprodukte/*Verbund-TOE*“ (3.25).

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 15408-1:2024-01

3.16
Klasse
<Taxonomie> Reihe von Familien mit einem gemeinsamen Fokus

Anmerkung 1 zum Begriff: Die Klasse wird weiter definiert in ISO/IEC 15408-2, die die Sicherheitsfunktionsklassen definiert, und ISO/IEC 15408-3, die die Vertrauenswürdigkeitsklassen definiert.

3.17
Komponente
<Taxonomie> kleinster selektierbarer Elementesatz, auf dem Anforderungen basieren können

3.18
Komponente
<Zusammensetzung> *Entität* (3.36), die Ressourcen und Dienstleistungen in einem Produkt bereitstellt

3.19
Komponenten-Evaluierungsgegenstand
Komponenten-TOE
(bewerteter) *Evaluierungsgegenstand (TOE)* (3.90), der Bestandteil eines anderen *zusammengesetzten TOEs* (3.21) ist

3.20
zusammengesetztes Vertrauenswürdigkeitspaket
CAP, en: composed assurance package
Vertrauenswürdigkeitspaket (3.7), bestehend aus Komponenten, die vorwiegend aus der ACO-*Klasse* (3.16) stammen und einen Punkt auf der vordefinierten Skala für zusammengesetzte Vertrauenswürdigkeit darstellen

3.21
zusammengesetzter Evaluierungsgegenstand
zusammengesetzter TOE
Evaluierungsgegenstand (TOE) (3.90), der ausschließlich aus zwei oder mehreren getrennt identifizierten Komponenten besteht, zwischen deren *TOE-Sicherheitsfunktionalitäten (TSF)* (3.92) eine Sicherheitsbeziehung besteht

Anmerkung 1 zum Begriff: Jede der separat identifizierten Komponenten ist selbst ein TOE.

3.22
zusammengesetzte Evaluierung
Evaluierung eines *zusammengesetzten TOE* (3.21) unter Verwendung der spezifischen, für zusammengesetzte TOE anwendbaren Evaluierungstechnik

Anmerkung 1 zum Begriff: Diese Evaluierungstechnik bezieht sich auf die ACO-Vertrauenswürdigkeits*klasse* (3.16), die in ISO/IEC 15408-3 definiert ist.

3.23
Verbundevaluation
Evaluierung eines *Verbund-TOE/-Produkts* (3.25) unter Verwendung der spezifischen Technik zur Verbundevaluation

Anmerkung 1 zum Begriff: Diese Evaluierungstechnik bezieht sich auf die COMP-bezogenen Vertrauenswürdigkeitsfamilien, die in ISO/IEC 15408-3 für die ADV-, ALC-, ASE-, ATE- und AVA-*Klassen* (3.16) festgelegt sind.

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-1:2024-01

3.24
Verbundprodukt
Produkt, das aus zwei oder mehr Komponenten besteht, die in zwei Schichten gegliedert werden können: eine Schicht mit einer bereits evaluierten Basis*komponente* (*Basis-TOE*) (3.15) und eine Schicht mit einer *abhängigen Komponente* (3.31)

3.25
Verbundevaluierungsgegenstand
Verbund-TOE
Teil eines *Verbundprodukts* (3.24), das den *Basis-TOE* (3.15) und die *abhängige Komponente* (3.31) enthält

Anmerkung 1 zum Begriff: Eine abhängige Komponente in einem Verbund-TOE kann aus einer oder mehreren abhängigen Komponenten bestehen. Zur Vereinfachung werden sie als „eine abhängige Komponente" betrachtet.

Anmerkung 2 zum Begriff: Ein Verbund-TOE kann Teile enthalten, die von der *Basiskomponente* (3.12) bzw. dem Basis-TOE unabhängig sind. Zur Vereinfachung werden solche Teile als zur abhängigen Komponente gehörig betrachtet.

Anmerkung 3 zum Begriff: Die *Verbundevaluation* (3.23) kann in einem inkrementellen Ansatz so oft wie nötig auf ein mehrkomponentiges/mehrschichtiges Produkt angewendet werden.

3.26
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 Compliance der festgelegten Anforderungen zu überprüfen

[QUELLE: ISO/IEC IEEE 24765:2017, 3.779 1]

3.27
Konfigurationsmanagementsystem
Satz von Verfahren und Werkzeugen (einschließlich deren Dokumentation), der von einem *Entwickler* (3.33) zur Entwicklung und Wartung der Konfigurationen der Produkte während ihrer Lebenszyklen verwendet wird

Anmerkung 1 zum Begriff: Konfigurationsmanagementsysteme können über unterschiedliche Stringenz- und Funktionsgrade verfügen. Auf den höheren Stufen können Konfigurationsmanagementsysteme automatisiert sein und über Mechanismen für die Mängelbehebung, Änderungskontrolle und sonstige Nachverfolgungsmechanismen verfügen.

3.28
abwehren, Verb
auf eine bestimmte Bedrohung reagieren, so dass die Bedrohung ausgemerzt oder abgemildert wird

3.29
nachweisliche Konformität
DC, en: demonstrable conformance
Beziehung zwischen einem *Schutzprofil* (PP) (3.68)/einer *Sicherheitsvorgabe* (3.82) (PP/ST) und einem PP oder zwischen einer ST und einer *PP-Konfiguration* (3.69), wobei das/die PP/ST eine gleichwertige oder restriktivere Lösung bietet, die das generische Sicherheitsproblem im PP/in der PP-Konfiguration löst

3.30
Abhängigkeit
Beziehung zwischen Komponenten, so dass ein *Schutzprofil (PP)* (3.68), eine *Sicherheitsvorgabe (ST)* (3.82), ein *Funktionspaket* (3.51) oder *Vertrauenswürdigkeitspaket* (3.7), das eine Komponente enthält, auch alle anderen Komponenten umfasst, die als abhängig ausgewiesen sind, oder eine Begründung enthält, warum sie es nicht sind

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-1:2024-01

3.31
abhängige Komponente
abhängige Entität (3.36) in einem Mehrkomponentenprodukt, die von der Bereitstellung von Dienstleistungen und Ressourcen durch eine oder mehrere *Basiskomponenten* (3.12) abhängt

Anmerkung 1 zum Begriff: Dies gilt insbesondere für „*zusammengesetzte TOE*“ (3.21) und „Verbundprodukte/*Verbund-TOE*“ (3.25).

3.32
abhängiger Evaluierungsgegenstand
abhängiger TOE
abhängige Komponente (3.31), die selbst Gegenstand einer Evaluierung ist

Anmerkung 1 zum Begriff: Dies gilt nur für „*zusammengesetzte TOE*“ (3.21) und nicht für „Verbundprodukte/*Verbund-TOE*“ (3.25).

3.33
Entwickler
Organisation, die für die Entwicklung des *Evaluierungsgegenstandes (TOE)* (3.90) verantwortlich ist

3.34
direkte Begründung
Art des *Schutzprofils* (3.68), des *PP-Moduls* (3.71) oder der *Sicherheitsvorgabe* (3.82), in denen die Elemente der *Sicherheitsproblemdefinition (SPD)* (3.80) direkt auf die *Sicherheitsfunktionsanforderungen (SFR)* (3.78) und möglicherweise auf die *Sicherheitszielsetzungen* (3.79) für die *Betriebsumgebung* (3.63) abgebildet werden

Anmerkung 1 zum Begriff: Die direkte Begründung enthält keine Sicherheitszielsetzungen für den *Evaluierungsgegenstand (TOE)* (3.90).

3.35
Element
<Taxonomie> in sich geschlossene Beschreibung eines Sicherheitsbedarfs, der einer *Vertrauenswürdigkeitsanforderung (SAR)* (3.76) oder einer *Sicherheitsfunktionsanforderung (SFR)* (3.78) zugeordnet ist

3.36
Entität
identifizierbarer Gegenstand, der durch einen Satz oder eine Sammlung von Eigenschaften beschrieben wird

Anmerkung 1 zum Begriff: Zu den Entitäten gehören Subjekte, Benutzer (einschließlich externer IT-Produkte), Objekte, Informationen, Sitzungen und/oder Ressourcen.

3.37
Evaluierung
Bewertung einer *PP-Konfiguration* (3.69), eines *Schutzprofils (PP)* (3.68), einer *Sicherheitsvorgabe (ST)* (3.82) oder eines *Evaluierungsgegenstandes (TOE)* (3.90) anhand definierter Kriterien

3.38
Evaluierungsaufgabe
EA
von einer oder mehreren Workunits abgeleitete Aufgabe

Anmerkung 1 zum Begriff: Die Workunits werden in ISO/IEC 18045 definiert.

Anmerkung 2 zum Begriff: Ableitungsmechanismen sind in ISO/IEC 15408-4 definiert.

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-1:2024-01

3.39
Vertrauenswürdigkeitsstufe
EAL-Stufe
EAL, en: evaluation assurance level
wohlgeformtes Paket aus *Vertrauenswürdigkeitsanforderungen* (3.76), das einen Punkt auf der vordefinierten Vertrauenswürdigkeitsskala darstellt

Anmerkung 1 zum Begriff: EAL werden in ISO/IEC 15408-5 definiert.

3.40
Evaluierungsinstanz
Stelle, die ein *Evaluierungsprogramm* (3.42) betreibt

Anmerkung 1 zum Begriff: Durch die Anwendung des Evaluierungsprogramms legt die Evaluierungsinstanz die Normen fest und überwacht die Qualität der Evaluierungen, die von Stellen innerhalb einer bestimmten Gemeinschaft durchgeführt werden.

3.41
Evaluierungsmethode
EM
Menge mit einer oder mehreren *Evaluierungsaufgaben* (3.38) zur Anwendung in einem bestimmten Kontext

3.42
Evaluierungsprogramm
Regeln, Verfahren und Management zur Durchführung von Evaluierungen der IT-Produktsicherheit

Anmerkung 1 zum Begriff: Ein Evaluierungsprogramm implementiert alle Teile der Normenreihe ISO/IEC 15408.

3.43
technischer Evaluierungsbericht
ETR, en: evaluation technical report
Dokumentation der *Gesamtentscheidung* (3.66) und ihrer Begründung, die vom *Evaluator* (3.45) erstellt und einer *Evaluierungsinstanz* (3.40) vorgelegt wird

3.44
technischer Evaluierungsbericht für Verbundevaluation
ETR für eine Verbundevaluation
ETR_COMP
Dokumentation, die im Rahmen des Ansatzes der *Verbundevaluation* (3.23) verwendet und vom *Evaluator* (3.45) der *Basiskomponente* (3.12) aus dem vollständigen *technischen Evaluierungsbericht (ETR)* (3.43) für die evaluierte Basiskomponente abgeleitet werden soll

Anmerkung 1 zum Begriff: Der ETR für die Verbundevaluation gehört zu der Basiskomponente und ihrer Evaluierung und wird für die Evaluierung eines Verbundprodukts mit einer solchen Basiskomponente verwendet, wenn der Ansatz der Verbundevaluation verwendet wird.

Anmerkung 2 zum Begriff: Der ETR für die Verbundevaluation in Bezug auf eine Basiskomponente ist so angelegt, dass er ausreichende Informationen für eine Verbundevaluation eines Verbundprodukts liefert, das eine solche bereits evaluierte Basiskomponente integriert. Er ermöglicht es dem *Evaluator* (3.45) des Verbundprodukts und der jeweiligen *Evaluierungsinstanz* (3.40) für das Verbundprodukt, die Angriffspfade und die Prüfungen, die für die Basiskomponente in Betracht gezogen und durchgeführt wurden, sowie die Wirksamkeit der von der Basiskomponente implementierten Gegenmaßnahmen zu verstehen.

AVA Documents Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-1:2024-01

3.45
Evaluator
Person, die mit der Durchführung von Evaluierungen nach einer bestimmten Evaluierungsnorm und der zugehörigen Evaluierungsmethodologie beauftragt ist

Anmerkung 1 zum Begriff: Ein Beispiel für Evaluierungsnormen ist die Normenreihe ISO/IEC 15408 mit der zugehörigen Evaluierungsmethodologie, die in ISO/IEC 18045 beschrieben ist.

[QUELLE: ISO/IEC 19896-1:2018, 3.5]

3.46
genaue Konformität
EC, en: exact conformance
hierarchische Beziehung zwischen einem *Schutzprofil (PP)* (3.68) oder einer *PP-Konfiguration* (3.69) und einer *Sicherheitsvorgabe (ST)* (3.82), wobei alle Anforderungen in der ST nur aus dem PP/der PP-Konfiguration abgeleitet sind

Anmerkung 1 zum Begriff: Eine ST darf eine genaue Konformität mit einem oder mehreren PP beanspruchen, aber nur mit einer PP-Konfiguration.

3.47
ausnutzbare Anfälligkeit
Schwachstelle im *Evaluierungsgegenstand (TOE)* (3.90), die für Verletzungen von *Sicherheitsfunktionsanforderungen (SFR)* (3.78) in der *Betriebsumgebung* (3.63) des TOEs genutzt werden kann

3.48
erweiterte Sicherheitsanforderung
Sicherheitsanforderung, die nach den Regeln in diesem Dokument entwickelt wurde, aber in keinem Teil der Normenreihe ISO/IEC 15408 aufgeführt ist

Anmerkung 1 zum Begriff: Eine erweiterte Sicherheitsanforderung behält die in ISO/IEC 15408-2 beschriebene Form und Syntax bei.

Anmerkung 2 zum Begriff: Erweiterte Sicherheitsanforderungen können von den Autoren von *Sicherheitsvorgaben (ST)* (3.82) oder *Schutzprofilen (PP)* (3.68) bzw. *PP-Modulen* (3.71) definiert werden.

3.49
externe Entität
Benutzer
menschliches technisches System oder eine seiner Komponenten, die mit dem *Evaluierungsgegenstand (TOE)* (3.90) von außerhalb der TOE-Grenze mit dem TOE interagiert

3.50
Familie
<Taxonomie> Satz von Komponenten, der eine ähnliche Zielsetzung hat, sich aber in Schwerpunkt oder Stringenz unterscheidet

3.51
Funktionspaket
benannter Satz von *Sicherheitsfunktionsanforderungen* (3.78), der von einer *Sicherheitsproblemdefinition (SPD)* (3.80) und von aus dieser SPD abgeleiteten *Sicherheitszielsetzungen* (3.79) begleitet sein kann

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-1:2024-01

3.52
gesamtes Vertrauenswürdigkeitspaket
Vertrauenswürdigkeitspaket (3.7), das für den gesamten *Evaluierungsgegenstand (TOE)* (3.90) bei einer *Evaluierung mit Mehrfach-Vertrauenswürdigkeit* (3.60) gilt

Anmerkung 1 zum Begriff: Das gesamtes Vertrauenswürdigkeitspaket kann erweiterte Vertrauenswürdigkeitskomponenten enthalten.

3.53
Leitliniendokumentation
Dokumentation, die die Auslieferung, die Bereitstellung, den Betrieb, das Management und/oder die Verwendung des *Evaluierungsgegenstands (TOE)* (3.90) beschreibt

3.54
Implementierungsrepräsentation
am wenigsten abstrakte Darstellung der *TOE-Sicherheitsfunktionalität (TSF)* (3.92), genauer die Darstellung, die ohne weitere Design*verfeinerung* (3.73) zur Erstellung der TSF selbst verwendet wird

Anmerkung 1 zum Begriff: Beispiele für Teile von Implementierungsrepräsentationen sind Quellcode, der anschließend kompiliert wird, oder Hardware-Zeichnungen, die zum Aufbau der eigentlichen Hardware verwendet werden.

3.55
in sich widerspruchsfrei, Adj.
es bestehen keine offensichtlichen Widersprüche zwischen irgendwelchen Aspekten einer *Entität* (3.36)

Anmerkung 1 zum Begriff: In Bezug auf Dokumentation bedeutet dies, dass keine Aussagen in der Dokumentation enthalten sein können, die als widersprüchlich zueinander interpretiert werden können.

3.56
Interpretation
Klärung oder Erweiterung einer Norm oder einer Anforderung an ein Evaluierungsprogramm

3.57
Iteration
Verwendung der gleichen Komponente, um zwei oder mehr unterschiedliche Anforderungen auszudrücken

3.58
Schichtung
Entwurfstechnik, bei der getrennte Komponentengruppen hierarchisch so organisiert sind, dass sie getrennte Zuständigkeiten besitzen, wobei eine Komponentengruppe die Dienste der in der Hierarchie darunterliegenden Komponentengruppen nutzt und die eigenen Dienste den darüberliegenden Komponentengruppen zur Verfügung stellt

3.59
Modul
architektonische Einheit, die auf einer für die Implementierung der Einheit geeigneten Ebene festgelegt ist

Anmerkung 1 zum Begriff: Die Eigenschaften im Zusammenhang mit der Aufteilung eines *Evaluierungsgegenstandes (TOE)* (3.90) in Module sind in ISO/IEC 15408-3 in den Familien ADV_TDS und ADV_INT beschrieben.

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-1:2024-01

3.60
Evaluierung mit Mehrfach-Vertrauenswürdigkeit
Evaluierung eines *Evaluierungsgegenstandes (TOE)* (3.90) unter Verwendung einer *PP-Konfiguration* (3.68), wobei jede PP-Konfigurationskomponente mit einem eigenen Satz von Vertrauenswürdigkeitsanforderungen verbunden ist

Anmerkung 1 zum Begriff: Mindestens eine der PP-Konfigurationskomponenten enthält einen abweichenden Satz von Vertrauenswürdigkeitsanforderungen als die anderen.

3.61
Objekt
Entität (3.36) im *Evaluierungsgegenstand (TOE)* (3.90), die Informationen enthält oder empfängt und an der Subjekte Operationen durchführen

3.62
Operation
<an einem Objekt> spezifische *Aktion* (3.1), die durch ein Subjekt an einem Objekt durchgeführt wird

3.63
Betriebsumgebung
Umgebung, in der der *Evaluierungsgegenstand (TOE)* (3.90) betrieben wird, bestehend aus allem, was sich außerhalb der TOE-Grenze befindet

3.64
optionale Sicherheitsfunktionsanforderung
optionale SFR
Sicherheitsfunktionsanforderung (SFR) (3.78) in einem *Schutzprofil (PP)* (3.68), *Funktionspaket* (3.51) oder *PP-Modul* (3.71), die zu einem bestimmten Aspekt der Beschreibung von Sicherheitsproblemen des PP beiträgt, deren Aufnahme in die Liste der SFR eines konformen PP oder der *Sicherheitsvorgaben* (*ST*) (3.82) jedoch nicht zwingend ist

Anmerkung 1 zum Begriff: Eine optionale SFR kann auf eine oder mehrere Bedrohungen der entsprechenden Elemente der *Sicherheitsproblemdefinition* (*SPD*) (3.80) und/oder organisatorische Sicherheitsrichtlinien (OSP) eingehen, die im Hauptteil des PP, des Funktionspakets oder des PP-Moduls angegeben sind, oder auf zugehörige SPD-Elemente/Zielsetzungen verweisen, die selbst optional sind (da sie nur durch die optionale SFR angesprochen werden).

3.65
organisatorische Sicherheitsrichtlinie
OSP, en: organisational security policy
Satz von Sicherheitsregeln, -verfahren oder -leitlinien für eine Organisation

Anmerkung 1 zum Begriff: Eine Richtlinie kann sich auf eine spezifische *Betriebsumgebung* (3.63) beziehen.

3.66
Gesamtentscheidung
Urteil, das ein *Evaluator* (3.45) hinsichtlich des Ergebnisses einer Evaluierung fällt

Anmerkung 1 zum Begriff: Das Urteil kann als „akzeptiert“ oder „abgelehnt“ ausgedrückt werden.

3.67
mögliche Anfälligkeit
vermutete, aber nicht bestätigte Schwachstelle

Anmerkung 1 zum Begriff: Der Verdacht ergibt sich aufgrund eines angenommenen Angriffspfads zur Verletzung der *Sicherheitsfunktionsanforderungen (SFR)* (3.78).

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-1:2024-01

3.68
Schutzprofil
PP, en: protection profile
implementierungsunabhängige Beschreibung der Sicherheitsanforderungen für einen Typ eines *Evaluierungsgegenstandes (TOE)* (3.90)

3.69
Schutzprofilkonfiguration
PP-Konfiguration
implementierungsunabhängige Beschreibung der Sicherheitsbedürfnisse für einen Typ eines *Evaluierungsgegenstandes (TOE)* (3.90), der mindestens ein *Schutzprofil (PP)* (3.68) und eine zusätzliche nicht leere Menge der PP und *PP-Module* (3.71) (mit den zugehörigen PP-Modulbasen) enthält

3.70
Konfigurationskomponente des Schutzprofils
PP-Konfigurationskomponente
Schutzprofil (PP) (3.68) oder *PP-Modul* (3.71), die in einer *PP-Konfiguration* (3.69) enthalten sind

3.71
Schutzprofilmodul
PP-Modul
implementierungsunabhängige Beschreibung der Sicherheitsbedürfnisse für einen Typ eines *Evaluierungsgegenstandes (TOE)* (3.90) ergänzend zu einem oder mehreren Basis*schutzprofilen* (3.68) und möglicherweise einigen Basis-PP-Modulen (3.14)

3.72
Modulbasis für das Schutzprofil
PP-Modulbasis
Satz entweder aus *PP-Modulen* (3.71) oder *Schutzprofilen (PP)* (3.68) oder aus beiden, festgelegt durch ein PP-Modul als Grundlage für die Erstellung einer *PP-Konfiguration* (3.69)

Anmerkung 1 zum Begriff: Der Begriff der PP-Modulbasis ist insofern iterativ, als die Basis eines PP-Moduls ein anderes PP-Modul mit einer eigenen Basis enthalten kann, wobei diese Basis ein PP-Modul enthält. Diese „Kette“ endet jedoch mit einem PP-Modul, das nur auf einem oder mehreren PP basiert.

3.73
Präzisierung
Hinzufügen von Details zu einer Sicherheitskomponente

3.74
Restanfälligkeit
Schwachstelle, die nicht in der *Betriebsumgebung* (3.63) des *Evaluierungsgegenstands (TOE)* (3.90) ausgenutzt werden kann, die aber für Verletzungen der *Sicherheitsfunktionsanforderungen (SFR)* (3.78) durch einen Angreifer genutzt werden kann, der ein höheres *Angriffspotential* (3.8) hat, als es für die Betriebsumgebung des TOEs angenommen wird

3.75
Rolle
vordefinierter Regelsatz, der die zulässigen Interaktionen zwischen einem Benutzer und dem *Evaluierungsgegenstand (TOE)* (3.90) festlegt

3.76
Vertrauenswürdigkeitsanforderung
SAR, en: security assurance requirement
Sicherheitsanforderung, die sich auf die Bedingungen und Prozesse für die Entwicklung und Lieferung des *Evaluationsgegenstands (TOE)* (3.90) und die von *Evaluatoren* (3.45) geforderten *Aktionen* (3.1) in Bezug auf die aus diesen Bedingungen und Prozessen resultierenden Nachweise bezieht

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-1:2024-01

3.77
Sicherheitsattribut
Eigenschaft von Subjekten, Benutzern, Objekten, Informationen, Sitzungen und/oder Ressourcen, die verwendet wird, um die *Sicherheitsfunktionsanforderungen (SFR)* (3.78) zu definieren, und deren Werte zur Durchsetzung der SFRs verwendet werden

Anmerkung 1 zum Begriff: Benutzer können externe IT-Produkte einschließen.

3.78
Sicherheitsfunktionsanforderung
SFR, en: security functional requirement
Sicherheitsanforderung, die zur Erfüllung der *Sicherheitsproblemdefinition (SPD)* (3.80) des *Evaluierungsgegenstands (TOE)* (3.90) beiträgt, wie in einer spezifischen *Sicherheitsvorgabe (ST)* (3.82) oder in einem *Schutzprofil (PP)* (3.68) definiert

Anmerkung 1 zum Begriff: Eine Sicherheitsfunktionsanforderung kann direkt behandelt werden, wie im Modell der *direkten Begründung* (3.34), oder indirekt durch die *Sicherheitszielsetzungen* (3.79) für den TOE, wie im allgemeinen Modell.

3.79
Sicherheitszielsetzung
Absichtserklärung, identifizierte Bedrohungen *abzuwehren* (3.28) und/oder identifizierte organisatorische Sicherheitsrichtlinien und/oder -annahmen zu erfüllen

3.80
Sicherheitsproblem
Sicherheitsproblemdefinition
SPD
Aussage, die formal die Natur und den Geltungsbereich der Sicherheit definiert, welche den *Evaluierungsgegenstand (TOE)* (3.90) adressieren soll

Anmerkung 1 zum Begriff: Diese Aussage besteht aus einer Kombination von: Bedrohungen, die durch den TOE und seine *Betriebsumgebung* (3.63) abgewehrt werden sollen, den organisatorischen Sicherheitsrichtlinien (OSP), die durch den TOE und seine Betriebsumgebung durchgesetzt, und den Annahmen, die für die Betriebsumgebung des TOE eingehalten werden.

Anmerkung 2 zum Begriff: SPD-Elemente umfassen Bedrohungen, OSP und Annahmen.

3.81
Sicherheitsanforderung
Anforderung, die Teil einer Sicherheitsspezifikation des *Evaluierungsgegenstands (TOE)* (3.90) ist, wie in einer spezifischen *Sicherheitsvorgabe (ST)* (3.82) oder in einem *Schutzprofil (PP)* (3.68) definiert

Anmerkung 1 zum Begriff: Die Anforderungen werden in einer Sprache, d. h. in Form und Syntax, angegeben, die in der Normenreihe ISO/IEC 15408 festgelegt ist.

3.82
Sicherheitsvorgabe
ST, en: Security Target
implementierungsabhängige Beschreibung der Sicherheitsanforderungen für einen *Evaluierungsgegenstand (TOE)* (3.90) auf der Grundlage einer *Sicherheitsproblemdefinition* (3.80)

3.83
Auswahl
Spezifikation eines oder mehrerer Element(e) aus einer Liste innerhalb einer Komponente

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-1:2024-01

3.84
auswahlbasierte Sicherheitsfunktionsanforderung
auswahlbasierte SFR
Sicherheitsfunktionsanforderung (SFR) (3.78) in einem *Schutzprofil (PP)* (3.78), *PP-Modul* (3.71) oder *Funktionspaket* (3.51), die zu einem bestimmten Aspekt der *Sicherheitsproblemdefinition* (3.80) des PP, PP-Moduls oder Funktionspakets beiträgt, das in ein(e) konforme(s) PP oder ST aufgenommen werden soll, wenn eine im PP/PP-Modul/Funktionspaket identifizierte Auswahlmöglichkeit anzeigt, dass sie eine zugehörige auswahlbasierte SFR hat

3.85
Evaluierung mit Einfach-Vertrauenswürdigkeit
Evaluierung eines *Evaluierungsgegenstandes (TOE)* (3.90) unter Verwendung eines Satzes von Vertrauenswürdigkeitsanforderungen

3.86
strikte Konformität
SC, en: strict conformance
hierarchische Beziehung zwischen einem *Schutzprofil (PP)* (3.68) und einem PP/einer *Sicherheitsvorgabe (ST)* (3.82), wobei alle Anforderungen im PP auch im PP/in der ST vorhanden sind

Anmerkung 1 zum Begriff: Diese Beziehung kann umschrieben werden als: „Die ST enthält alle Aussagen, die im PP vorhanden sind, kann aber weitere enthalten“. Es wird erwartet, dass strikte Konformität für stringente Anforderungen eingesetzt wird, die in konsistenter Weise erfüllt werden müssen.

3.87
Teil-TOE-Sicherheitsfunktionalität
Teil-TSF
kombinierte Funktionalität der gesamten Hardware, Software und Firmware eines *Evaluierungsgegenstands (TOE)* (3.90), auf die sich die korrekte Durchsetzung der in einer *PP-Konfigurationskomponente* (3.69) definierten Sicherheitsfunktionsanforderungen (SFR) stützt

Anmerkung 1 zum Begriff: Dieser Satz von SFR wird durch Abhängigkeiten, Zielsetzungen und Elemente der *Sicherheitsproblemdefinition (SPD)* (3.80) in der PP-Konfigurationskomponente geschlossen.

Anmerkung 2 zum Begriff: Der Begriff der Teil-TSF wird im Zusammenhang mit der Spezifikation und Evaluierung von PP-Konfigurationen und konformen Sicherheitsvorgaben (ST) verwendet. Sie kann im Ansatz mit Einfach-Vertrauenswürdigkeit verwendet werden, muss aber im Ansatz mit Mehrfach-Vertrauenswürdigkeit verwendet werden: Teil-TSF müssen in einer PP-Konfiguration mit Mehrfach-Vertrauenswürdigkeit und in konformen ST mit Mehrfach-Vertrauenswürdigkeit definiert werden.

Anmerkung 3 zum Begriff: Jede Teil-TSF ist mit einem eigenen Satz von Vertrauenswürdigkeitsanforderungen (SAR) in einer PP-Konfiguration/ST mit Mehrfach-Vertrauenswürdigkeit verbunden. Im weiteren Verlauf des Dokuments kann ein Satz von SAR ein *Vertrauenswürdigkeitspaket* (3.7) darstellen.

Anmerkung 4 zum Begriff: Eine Teil-TSF hat die Merkmale einer TSF.

3.88
Subjekt
Entität (3.36) im *Evaluierungsgegenstand (TOE)* (3.90), die Operationen an Objekten durchführt

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 15408-1:2024-01

3.89
Anpassung
Hinzufügung einer oder mehrerer funktionaler Anforderungen zu einem *Funktionspaket* (3.51) und/oder Hinzufügung einer oder mehrerer Auswahlen zu einer *Sicherheitsfunktionsanforderung (SFR)* (3.78) in einem Funktionspaket

Anmerkung 1 zum Begriff: Eine solche Anpassung wird nur im Zusammenhang mit einem Paket betrachtet und nicht im Zusammenhang mit anderen Paketen oder *Schutzprofilen (PP)* (3.68) bzw. PP-Modulen.

Anmerkung 2 zum Begriff: Die Auswahlen in der SFR können durch die zusätzlichen Auswahlen ersetzt werden.

Anmerkung 3 zum Begriff: Auswahlen können nur für Pakete hinzugefügt werden, die von den PP oder PP-Modulen beansprucht werden. Die ST können keine an das Paket angepasste Konformität mit dem Paketnamen beanspruchen.

3.90
Evaluierungsgegenstand
TOE, en: target of evaluation
Satz aus Software, Firmware und/oder Hardware, möglicherweise mit beigefügten Leitlinien, der Gegenstand einer Evaluierung ist

3.91
Bedrohungsagent
Entität (3.36), die das Potential hat, nachteilige *Aktionen* (3.3) auf *Vermögenswerte* (3.4) auszuüben, die durch den *Evaluierungsgegenstand (TOE)* (3.90) geschützt sind

3.92
TOE-Sicherheitsfunktionalität
TSF, en: TOE security functionality
kombinierte Funktionalität der gesamten Hardware, Software und Firmware eines *Evaluierungsgegenstands (TOE)* (3.90), auf die sich die korrekte Durchsetzung der *Sicherheitsfunktionsanforderungen (SFR)* (3.78) stützt

3.93
TOE-Typ
Satz von Merkmalen, die einer Gruppe von *Evaluierungsgegenständen (TOE)* (3.90) gemeinsam sind

Anmerkung 1 zum Begriff: Der TOE-Typ kann in einem *Schutzprofil (PP)* (3.68) expliziter definiert werden.

3.94
Übersetzung
Prozess der Beschreibung von Sicherheitsanforderungen in einer standardisierten Sprache

Anmerkung 1 zum Begriff: Die Verwendung des Begriffs „Übersetzung“ ist in diesem Zusammenhang nicht wörtlich zu nehmen; es wird nicht impliziert, dass jede in standardisierter Sprache ausgedrückte *Sicherheitsfunktionsanforderung (SFR)* (3.78) wieder in die *Sicherheitszielsetzungen* (3.79) zurückübersetzt werden kann.

3.95
Anfälligkeit
Schwachstelle im *Evaluierungsgegenstand (TOE)* (3.90), die für Verletzungen von *Sicherheitsfunktionsanforderungen (SFR)* (3.78) in manchen Umgebungen ausgenutzt werden kann

4 Symbole und Abkürzungen

AP	Vertrauenswürdigkeitspaket (en: Assurance Package)
API	Anwendungsprogrammierschnittstelle (en: Application Programming Interface)
CAP	zusammengesetztes Vertrauenswürdigkeitspaket (en: Composed Assurance Package)

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-1:2024-01

CD	Compact Disc
CM,	Konfigurationsmanagement (en: Configuration Management)
COMP	Vertrauenswürdigkeitspaket für Verbundprodukte (en: Composed Product Assurance Package)
DAC	benutzerbestimmbare Zugangssteuerung (en: Discretionary Access Control)
DC	nachweisliche Konformität (en: Demonstrable Conformance)
DPA	differentielle Stromverbrauchsanalyse (en: Differential Power Analysis)
DRBG	deterministischer Zufallsbitgenerator (en: Deterministic Random Bit Generator)
EA	Evaluierungsaufgabe
EAL	Vertrauenswürdigkeitsstufe (en: Evaluation Assurance Level)
EC	genaue Konformität (en: exact conformance)
EM	Evaluierungsmethode
EMS	elektromagnetisches Spektrum
ETR	technischer Evaluierungsbericht (en: Evaluation Technical Report)
GAP	gesamtes Vertrauenswürdigkeitspaket (en: Global Assurance Package)
GB	Gigabyte
GHz	Gigahertz
GUI	grafische Benutzungsschnittstelle (en: Graphical User Interface)
HSM	Hardware-Sicherheitsmodul
HTTPS	Hypertext-Übertragungsprotokoll sicher (en: Hypertext Transfer Protocol Secure)
IC	integrierte Schaltung (en: Integrated Circuit)
IOCTL	Eingabe-Ausgabe-Steuerung (en: Input Output Control)
IP	Internet-Protokoll
IPsec	IP-Sicherheit (Protokoll) (en: IP security)
IT	Informationstechnologie
LDAP	vereinfachtes Verzeichniszugriffsprotokoll (en: Lightweight Directory Access Protocol)
MAC	systembestimmte Zugangssteuerung (en: Mandatory Access Control)
MB	Megabyte
MBps	Megabytes je Sekunde
OR	Beobachtungsbericht (en: Observation Report)
OS	Betriebssystem (en: Operating System)
OSP	organisatorische Sicherheitsrichtlinie (en: Organisational Security Policy)
OTP	einmalig programmierbar (en: One-Time Programmable)
PC	Personal Computer
PCI	Peripheral Component Interconnect
PKI	Public-Key-Infrastruktur (en: Public Key Infrastructure)
PP	Schutzprofil (en: Protection Profile)
PPA	Vertrauenswürdigkeitspaket für das Schutzprofil (en: Protection Profile Assurance package)
RAM	Direktzugriffsspeicher (en: Random Access Memory)
RBG	Zufallsbitgenerator (en: Random Bit Generator)
RNG	Zufallszahlengenerator (en: Random Number Generator)
RPC	Remote Procedure Call
SAR	Vertrauenswürdigkeitsanforderung (en: Security Assurance Requirement)
SC	strikte Konformität (en: Strict Conformance)

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-1:2024-01

SFP	Sicherheitsfunktionsrichtlinien (en: Security Function Policies)
SFR	Sicherheitsfunktionsanforderung (en: Security Functional Requirement)
SPA	einfache Stromverbrauchsanalyse (en: Simple Power Analysis)
SPD	Sicherheitsproblemdefinition (en: Security Problem Definition)
SSH	Secure Shell
ST	Sicherheitsvorgabe (en: Security Target)
STA	Vertrauenswürdigkeitspaket für die Sicherheitsvorgabe (En: Security Target Assurance package)
TCP	Transmission Control Protocol
TLS	Transportschichtsicherheit (en: Transport Layer Security)
TOE	Evaluierungsgegenstand (en: target of evaluation)
TSF	TOE-Sicherheitsfunktionalität (en: TOE Security Functionality)
TSFI	TSF-Schnittstelle (en: TSF Interface)
USB	universeller serieller Bus
VPN	Virtual Private Network

5 Übersicht

5.1 Allgemein

In diesem Abschnitt werden die wesentlichen Konzepte der Normenreihe ISO/IEC 15408 eingeführt. Beschrieben werden das Konzept des Evaluierungsgegenstands (TOE), die Zielgruppe der Normenreihe ISO/IEC 15408 und die Art der Präsentation des Inhalts in der Normenreihe ISO/IEC 15408.

5.2 Beschreibung der Normenreihe ISO/IEC 15408

5.2.1 Allgemein

Wie unten aufgezeigt, wird die Normenreihe ISO/IEC 15408 als eine Reihe eigenständiger aber zusammenhängender Teile dargestellt:

a) **ISO/IEC 15408-1, Einleitung und allgemeines Modell** ist die Einleitung zur Normenreihe ISO/IEC 15408. Dieser Teil definiert die allgemeinen Konzepte und Grundlagen der IT-Sicherheitsevaluierung und zeigt ein allgemeines Evaluierungsmodell;

b) **ISO/IEC 15408-2, Sicherheitsfunktionskomponenten** legt einen Satz an Funktionskomponenten als Standardvorlagen fest, die als Grundlage für Sicherheitsfunktionsanforderungen (SFR) an TOEs dienen. ISO/IEC 15408-2 katalogisiert den Satz an Sicherheitsfunktionskomponenten und organisiert ihn in Familien und Klassen;

c) **ISO/IEC 15408-3, 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. ISO/IEC 15408-3 legt auch Evaluierungskriterien für die PP, ST und TOE fest;

d) **ISO/IEC 15408-4, „Rahmen für die Festlegung von Bewertungsmethoden und -tätigkeiten“** bietet einen normgerechten Rahmen für die Spezifikation von Evaluierungsmethoden und -aufgaben, die in den PP, ST und allen sie unterstützenden Dokumenten enthalten sein können, um von Evaluatoren zur Unterstützung von Evaluierungen unter Verwendung des in den anderen Teilen der Normenreihe ISO/IEC 15408 beschriebenen Modells verwendet zu werden. ISO/IEC 18045 ist grundlegend für ISO/IEC 15408-4;

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-1:2024-01

e) **ISO/IEC 15408-5, „Vordefinierte Pakete von Sicherheitsanforderungen“** stellt Vertrauenswürdigkeitspakete und SFR zur Verfügung, die als zweckmäßig zur Unterstützung der gemeinsamen Nutzung durch die interessierten Parteien identifiziert worden sind. Beispiele für bereitgestellte Pakete umfassen die Vertrauenswürdigkeitsstufen (EAL-Stufen) und die zusammengesetzten Vertrauenswürdigkeitspakete (CAP).

Bei der Anwendung der Normenreihe ISO/IEC 15408 muss eine Begründung vorgelegt werden, wenn die empfohlene Option nicht gewählt wird.

Zur Unterstützung der Normenreihe ISO/IEC 15408 wurden noch weitere Dokumente veröffentlicht. In den Literaturhinweisen sind Dokumente zur Unterstützung aufgeführt.

ANMERKUNG ISO/IEC 18045 umfasst die grundlegende Methodologie für IT-Sicherheitsevaluierungen, die in Übereinstimmung mit der Normenreihe ISO/IEC 15408 durchgeführt wird.

5.2.2 Zielgruppe

5.2.2.1 Allgemein

Fünf Hauptgruppen haben ein allgemeines Interesse an der Evaluierung der Sicherheitseigenschaften der TOE: Verbraucher (Risikoeigentümer), Entwickler, technische Arbeitsgruppen, Evaluatoren und andere. Die in der Normenreihe ISO/IEC 15408 enthaltenen Informationen wurden so strukturiert, dass sie die Bedürfnisse all dieser Gruppen abdecken, die als Hauptbenutzer der Normenreihe ISO/IEC 15408 angesehen werden. In 5.2.2.2 bis 5.2.2.6 wird erklärt, wie die Gruppen von den Kriterien profitieren können.

5.2.2.2 Verbraucher (Risikoeigentümer)

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

Risikoeigentümer 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. Risikoeigentümer können die Evaluierungsergebnisse auch verwenden, um verschiedene TOEs zu vergleichen.

Die Normenreihe ISO/IEC 15408 übergibt Risikoeigentümern, insbesondere jenen in Verbrauchergruppen und Interessengemeinschaften, eine implementationsunabhängige Struktur, das sogenannte PP, in dem ihre Sicherheitsanforderungen eindeutig formuliert werden können.

5.2.2.3 Entwickler

Die Normenreihe ISO/IEC 15408 ist für die Unterstützung von IT-Produktentwicklern 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 taget) enthalten. Diese ST kann einem oder mehreren PPs entsprechen, um aufzuzeigen, dass der TOE die Sicherheitsanforderungen von Verbrauchern erfüllt, die in jenen PPs dargelegt sind.

Die Normenreihe 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.

5.2.2.4 Technische Arbeitsgruppen

Die Normenreihe ISO/IEC 15408 soll technische Arbeitsgruppen bei der Vorbereitung und Entwicklung der PP, PP-Module, PP-Konfigurationen, Pakete und unterstützenden Dokumente oder Leitlinien unterstützen. Technische Arbeitsgruppen können sich aus interessierten Parteien wie Verbrauchern (Risikoeigentümern), Entwicklern, Evaluatoren und Wissenschaftlern zusammensetzen.

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-1:2024-01

5.2.2.5 Evaluatoren

Die Normenreihe ISO/IEC 15408 enthält Kriterien, die von Evaluatoren bei ihrer Beurteilung zur Konformität von TOEs, ST, PP und PP-Konfigurationen mit ihren Sicherheitsanforderungen zu verwenden sind. Die Normenreihe ISO/IEC 15408 beschreibt die allgemeine Reihe von Aktionen, die von Evaluatoren auszuführen sind.

ANMERKUNG Die Normenreihe ISO/IEC 15408 spezifiziert keine Verfahren zur Ausführung dieser Aktionen. Weitere Informationen zu diesen Verfahren können Abschnitt 13 entnommen werden.

5.2.2.6 Weitere

Die Normenreihe 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 Normenreihe 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;

f) Evaluierungsinstanzen, die für das Management und die Aufsicht eines IT-Sicherheitsevaluierungsprogramms verantwortlich sind;

g) Akademiker, die Forschung zum Thema IT-Sicherheit betreiben.

Tabelle 1 zeigt, wie die einzelnen Teile der Normenreihe ISO/IEC 15408 für jede der Zielgruppen von Interesse sein können.

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-1:2024-01

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

Teile der ISO/IEC 15408	Verbraucher (Risikoeigentümer)	Entwickler	Technische Arbeitsgruppen	Evaluatoren	Weitere
Teil 1	Sollte für Hintergrundinformationen, Verweisungszwecke und als Leitfaden für die Struktur der PP, PP-Module, PP-Konfigurationen, ST und Zusammensetzung verwendet werden. Muss für die Entwicklung von Sicherheitsspezifikationen und Sicherheitsproblemdefinitionen (SPD) für TOE verwendet werden.	Sollte für Hintergrundinformationen, Verweisungszwecke und als Leitfaden für die Struktur der PP, PP-Module, PP-Konfigurationen, ST und Zusammensetzung verwendet werden. Muss für die Entwicklung von Sicherheitsspezifikationen für TOEs verwendet werden.	Sollte für Hintergrundinformationen, Verweisungszwecke und als Leitfaden für die Struktur der PP, PP-Module, PP-Konfigurationen, ST und Zusammensetzung verwendet werden. Muss für die Entwicklung von Sicherheitsspezifikationen für Pakete, PP, PP-Module und PP-Konfigurationen verwendet werden.	Sollte für Hintergrundinformationen, Verweisungszwecke und als Leitfaden für die Struktur der PP, PP-Module, PP-Konfigurationen, ST und Zusammensetzung verwendet werden. Muss bei der Evaluierung der PP, PP-Konfigurationen und ST verwendet werden.	Darf für Hintergrundinformationen, Verweisungszwecke und als Leitfaden für die Struktur der PP, PP-Module, PP-Konfigurationen, ST und Zusammensetzung verwendet werden.
Teil 2	Muss als Leitfaden und zur Verweisung bei der Festlegung von Aussagen zu Sicherheitsfunktionskomponenten für deren Risikoumgebung verwendet werden.	Muss zur Verweisung bei der Interpretation von Aussagen zu Sicherheitsfunktionskomponenten in Paketen, PP und PP-Modulen verwendet werden. Muss bei der Ausarbeitung der ST verwendet werden. Darf bei der Formulierung von Sicherheitsfunktionen für IT-Produkte verwendet werden.	Muss zur Verweisung bei der Festlegung von Aussagen zu Sicherheitsfunktionskomponenten in Paketen, PP und PP-Modulen verwendet werden.	Muss zur Verweisung bei der Evaluierung von Sicherheitsfunktionskomponenten in Paketen, PP und PP-Modulen oder Sicherheitsfunktionsanforderungen (SFR) in den ST verwendet werden.	Darf zur Verweisung bei der Überprüfung der in den Paketen, PP und PP-Modulen angegebenen Sicherheitsfunktionskomponenten oder der Sicherheitsfunktionsanforderungen (SFR) in den ST verwendet werden.
Teil 3	Muss als Leitlinien und zur Verweisung bei der Bestimmung der für ihre Risikoumgebung erforderlichen Sicherheitsmaßnahmen verwendet werden.	Muss zur Verweisung bei der Interpretation von Aussagen zu Vertrauenswürdigkeitskomponenten in Paketen, PP, PP-Modulen und PP-Konfigurationen verwendet werden. Muss bei der Ausarbeitung der ST verwendet werden. Darf bei der Formulierung oder Verbesserung der Entwicklungsprozesse verwendet werden.	Muss zur Verweisung bei der Festlegung von Aussagen zu Vertrauenswürdigkeitskomponenten in Paketen, PP, PP-Modulen und PP-Konfigurationen verwendet werden.	Muss zur Verweisung bei der Evaluierung von Sicherheitsfunktionskomponenten in Paketen, PP, PP-Modulen und PP-Konfigurationen oder Vertrauenswürdigkeitsanforderungen in den ST verwendet werden.	Darf zur Verweisung bei der Überprüfung der in den Paketen, PP, PP-Modulen und PP-Konfigurationen angegebenen Sicherheitsfunktionskomponenten oder der Vertrauenswürdigkeitsanforderungen in den ST verwendet werden.

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 15408-1:2024-01

Tabelle 1 (*fortgesetzt*)

Teile der ISO/IEC 15408	Verbraucher (Risikoeigentümer)	Entwickler	Technische Arbeitsgruppen	Evaluatoren	Weitere
Teil 4	Sollte zur Verweisung und Hintergrundinformation für die Struktur der Evaluierungsmethode(n) und/oder -aufgaben verwendet werden.	Sollte zu Referenzzwecken und als Leitlinien für die Struktur der Evaluierungsmethode(n) und/oder -aufgaben verwendet werden.	Sollte zu Referenzzwecken und als Leitlinien für die Struktur der Evaluierungsmethoden und -aufgaben verwendet werden.	Sollte zu Referenzzwecken und als Leitlinien für die Struktur der Evaluierungsmethoden und -aufgaben verwendet werden. Sollte bei der Formulierung spezifischer Evaluierungsmethoden und -aufgaben verwendet werden.	Darf zu Referenzzwecken und als Leitlinien für die Struktur der Evaluierungsmethoden und -aufgaben verwendet werden.
Teil 5	Sollte zur Verweisung bei der Bestimmung des Inhalts von beanspruchten vordefinierten Paketen von Sicherheitsanforderungen verwendet werden.	Muss bei der Entwicklung der ST verwendet werden, die Konformität mit vordefinierten Paketen von Sicherheitsanforderungen beanspruchen. Muss zur Verweisung bei der Vorbereitung eines TOE für die Evaluierung konform mit vordefinierten Paketen von Sicherheitsanforderungen verwendet werden.	Muss bei der Entwicklung der PP, PP-Module und PP-Konfigurationen verwendet werden, die Konformität mit vordefinierten Paketen von Sicherheitsanforderungen beanspruchen.	Muss zur Verweisung bei der Evaluierung der PP, PP-Module und PP-Konfigurationen oder ST verwendet werden, die Konformität mit vordefinierten Paketen von Sicherheitsanforderungen beanspruchen.	Darf zur Verweisung bei der Bestimmung des Inhalts von beanspruchten vordefinierten Paketen von Sicherheitsanforderungen verwendet werden.

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-1:2024-01

5.3 Evaluierungsgegenstand (TOE)

5.3.1 Allgemein

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

Der TOE mag in vielen Fällen ein vollständiges 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 Normenreihe 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.

BEISPIEL Beispiele für TOE sind Geräte, die sich durch wenige Schnittstellen, eine geringe Angriffsfläche und eine bekannte Lieferkette auszeichnen:

— ein Netzwerkgerät;

— eine Softwareanwendung;

— ein Betriebssystem;

— ein Virtualisierungssystem;

— eine integrierte Schaltung;

— der kryptographische Co-Prozessor einer integrierten Schaltung;

— eine Anwendung für ein Mobilgerät;

— eine Datenbankanwendung ohne Remote-Client-Software, die bei Datenbankanwendungen üblich ist.

Die TOE können auch komplexer sein, gekennzeichnet durch eine große Schnittstelle/große Schnittstellen und/oder eine große Anzahl an Komponenten, mehrere Herstellungs-/Integrationsphasen, vor Ort aufrüstbare Produkte wie z. B.:

— ein lokales Netz (LAN) mit allen Terminals, Servern, Netzwerkeinrichtungen und Software;

— ein Mobilgerät;

— Gateways und Hubs;

— eine Softwareanwendung in Verbindung mit einem Betriebssystem;

— ein Multifunktionsgerät wie z. B. einen Multifunktionsdrucker;

— ein Hardware-Sicherheitsmodul (HSM).

5.3.2 TOE-Grenzen

Das Konzept einer TOE-Grenze ist für die Spezifikation der ST von grundlegender Bedeutung.

Ein TOE kann ein komplettes IT-Produkt (oder Produkte) sein, ein Teil eines IT-Produkts oder aus verschiedenen Komponenten bestehen. Die ST muss den physischen und logischen Anwendungsbereich des TOE bei der Auslieferung an den Kunden klar umreißen.

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-1:2024-01

Alle Teile eines IT-Produkts, die nicht innerhalb der TOE-Grenze liegen, befinden sich außerhalb des Anwendungsbereichs der Evaluierung und werden als *Nicht-TOE-Teile des IT-Produkts* bezeichnet.

5.3.3 Unterschiedliche Darstellungen des TOEs

In der Normenreihe ISO/IEC 15408 kann ein TOE im Zusammenhang mit den Vertrauenswürdigkeitskriterien in mehreren Darstellungen auftreten:

ANMERKUNG Zu diesen Vertrauenswürdigkeitskriterien gehören das Prüfen (ATE) und die Anfälligkeitsanalyse (AVA), für die Proben des TOE erforderlich sind, einige Designkriterien (ADV_IMP), für die eine Implementierungsrepräsentation, z. B. der Quellcode, erforderlich ist, und der Lebenszyklus (ALC), für den die Konfigurationsliste des TOE erforderlich ist.

BEISPIEL TOE-Darstellungen für einen Software-TOE:

— eine Liste von Dateien in einem Konfigurationsmanagementsystem;

— eine einzige Master-Kopie, die soeben kompiliert wurde;

— der Quellcode für eine bestimmte Version einer Open-Source-Distribution;

— eine Schachtel mit einem physischen Medium und einem Handbuch, bereit zur Lieferung an den Kunden;

— eine Binärdatei, die zum sicheren Download bereitsteht;

— eine installierte und betriebsbereite Version.

TOE-Darstellungen für einen Hardware-TOE:

— Layout von integrierten Schaltungen;

— Speicherzuordnungen;

— Wafer;

— Module.

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

5.3.4 Unterschiedliche Konfigurationen des TOEs

Im Allgemeinen können IT-Produkte auf unterschiedliche Weise mit verschiedenen aktivierten oder deaktivierten Optionen konfiguriert werden. Bei einer Evaluierung, die in Übereinstimmung mit der Normenreihe ISO/IEC 15408 durchgeführt wird, wird festgestellt, ob ein TOE bestimmte Anforderungen erfüllt. Es ist oft der Fall, dass der Leitlinienteil des TOE die möglichen Konfigurationen des TOE einschränkt, d. h. die Leitlinien für den TOE können sich von den allgemeinen Leitlinien des IT-Produkts unterscheiden.

BEISPIEL Ein Betriebssystem ist ein IT-Produkt: Das Produkt kann auf verschiedene Arten konfiguriert werden, einschließlich z. B. der Arten der Benutzer, der Anzahl der Benutzer, der Arten der erlaubten/unerlaubten externen Verbindungen, der aktivierten/deaktivierten Optionen.

Wenn ein IT-Produkt einen TOE enthält oder ein TOE ist, muss die Konfiguration des Produkts im Allgemeinen sehr viel strenger kontrolliert werden, da einige Konfigurationsoptionen dazu führen können, dass ein TOE die Anforderungen nicht erfüllt.

Aus diesem Grund wäre ein Unterschied zu erwarten zwischen der Leitliniendokumentation für das allgemeine IT-Produkt, die viele Konfigurationen zulässt, und der Leitliniendokumentation für den TOE, die möglicher-

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-1:2024-01

weise nur eine oder nur eine Reihe von Konfigurationen zulässt, die sich in sicherheitsrelevanter Hinsicht nicht unterscheiden.

Wenn die Leitliniendokumentation für den TOE mehr als eine Konfiguration erlaubt, werden diese Konfigurationen insgesamt „der TOE“ genannt, und jede Konfiguration muss die an den TOE gestellten Anforderungen erfüllen.

5.3.5 Betriebsumgebung des TOE

Alles, was außerhalb der TOE-Grenze liegt, gehört zur Betriebsumgebung des TOE. Wenn der TOE-Teil eines IT-Produkts ist, kann das IT-Produkt Teile haben, die nicht zum TOE gehören. Solche Nicht-TOE-Teile sind ebenfalls Teil der Betriebsumgebung des TOE.

Die ST muss Annahmen beschreiben und Sicherheitszielsetzungen für die Betriebsumgebung definieren, die zusammen mit der vom TOE selbst bereitgestellten Sicherheitsfunktionalität notwendig sind, um die Bedrohungen abzuschwächen und die organisatorischen Sicherheitsrichtlinien (OSP) durchzusetzen.

Die Sicherheitszielsetzungen für die Betriebsumgebung dürfen die TOE-Sicherheitsfunktionalität unterstützen.

Die ST muss klare Anforderungen an die TOE-Umgebung formulieren, um dem Benutzer ausreichende Informationen für die ordnungsgemäße Nutzung des evaluierten TOE zur Verfügung zu stellen.

BEISPIEL Beispiele für eine Sicherheitszielsetzung für die Betriebsumgebung, die die kryptographischen Dienste des TOE unterstützt, die unter Verwendung der FCS-Komponenten von ISO/IEC 15408-2 festgelegt wurden, sind sichere Schlüsselgenerierungs- und Injektionsvoraussetzungen und -prozesse.

5.4 Darstellung des Inhalts dieses Dokuments

Das allgemeine Modell wird in Abschnitt 6 vorgestellt, in dem die Konzepte im Zusammenhang mit der Evaluierung der Sicherheitsfunktionalität von IT-Produkten, der Definition des Sicherheitsproblems und der Spezifikation von Sicherheitsanforderungen zur Lösung des Sicherheitsproblems erläutert werden. Es werden Konzepte für die Spezifikation von Sicherheitsanforderungen, Paketen, PP, PP-Modulen und PP-Konfigurationen vorgestellt, die sich auf die Bedürfnisse von Risikoeigentümern mit ähnlichen Sicherheitsproblemen beziehen.

Die in ISO/IEC 15408-2 und ISO/IEC 15408-3 vorgesehenen Mittel zur Spezifizierung von Sicherheitsanforderungen und zur Vervollständigung von Sicherheitskomponenten werden in Abschnitt 7 und Abschnitt 8 erläutert.

Die Anforderungen und Empfehlungen für die Kernkonstrukte der Pakete, PP, PP-Module, PP-Konfigurationen und ST sind in Abschnitt 9, Abschnitt 10, Abschnitt 11 und 11.3.3 erläutert.

Die Anforderungen und Empfehlungen für die Evaluierung und die Evaluierungsergebnisse für die TOE, ST, PP und PP-Konfigurationen sind in Abschnitt 13 zu finden.

Schließlich findet sich das Thema der Zusammensetzung der Vertrauenswürdigkeit in Abschnitt 14.

6 Allgemeines Modell

6.1 Hintergrund

Dieser Abschnitt zeigt die durchgängig in der Normenreihe ISO/IEC 15408 verwendeten allgemeinen Konzepte, einschließlich des Kontextes, in dem die Konzepte zu verwenden sind, und des Ansatzes zur Anwendung der Konzepte. ISO/IEC 15408-2, ISO/IEC 15408-3, ISO/IEC 15408-4 und ISO/IEC 15408-5 erweitern die Verwendung dieser Konzepte und gehen davon aus, dass der hier beschriebene Ansatz verwendet wird. Des Weiteren ist ISO/IEC 18045 anwendbar für Anwender der Normenreihe ISO/IEC 15408, die Evaluierungstätigkeiten planen.

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-1:2024-01

Die Normenreihe 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 Normenreihe ISO/IEC 15408. Die Konzepte selbst sind allerdings nicht dazu ausgelegt, die Klassen der IT-Sicherheitsprobleme einzuschränken, für die die Normenreihe ISO/IEC 15408 anwendbar ist. Abschnitt 6 setzt voraus, dass der Leser über Wissen im Bereich der IT-Sicherheit verfügt, und er soll nicht als Anleitung in diesem Bereich dienen.

6.2 Vermögenswerte und Sicherheitsmaßnahmen

Bei der Sicherheit geht es um den Schutz von Vermögenswerten innerhalb der Betriebsumgebung.

BEISPIEL 1 Ein Beispiel für einen Vermögenswert sind Inhalte von Dateien oder eines Servers.

Beispiele für Betriebsumgebungen im Zusammenhang mit einem solchen Vermögenswert sind:

— ein Rechenzentrum, in dem der Server installiert ist;

— ein mit dem Internet verbundenes Rechnernetzwerk, das den Server mit der Welt verbindet;

— ein LAN, das den Server mit anderen Servern und/oder Arbeitsstationen verbindet;

— die alltägliche Umgebung eines Benutzers, der Informationen vom Server oder eine bestimmte Datei verwendet;

— eine allgemeine Büroumgebung, die Kommunikationsmöglichkeiten mit dem Server und/oder einer bestimmten Datei bietet.

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 in der Betriebsumgebung implementierten Sicherheitsmaßnahmen vor Bedrohungen geschützt werden. Bild 1 zeigt diese übergeordneten Konzepte und Beziehungen.

ANMERKUNG ISO/IEC 27001 bietet die Anforderungen für die Einrichtung, Umsetzung, Aufrechterhaltung und fortlaufende Verbesserung eines Informationssicherheitsmanagementsystems einschließlich der Spezifikation der Maßnahmen.

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-1:2024-01

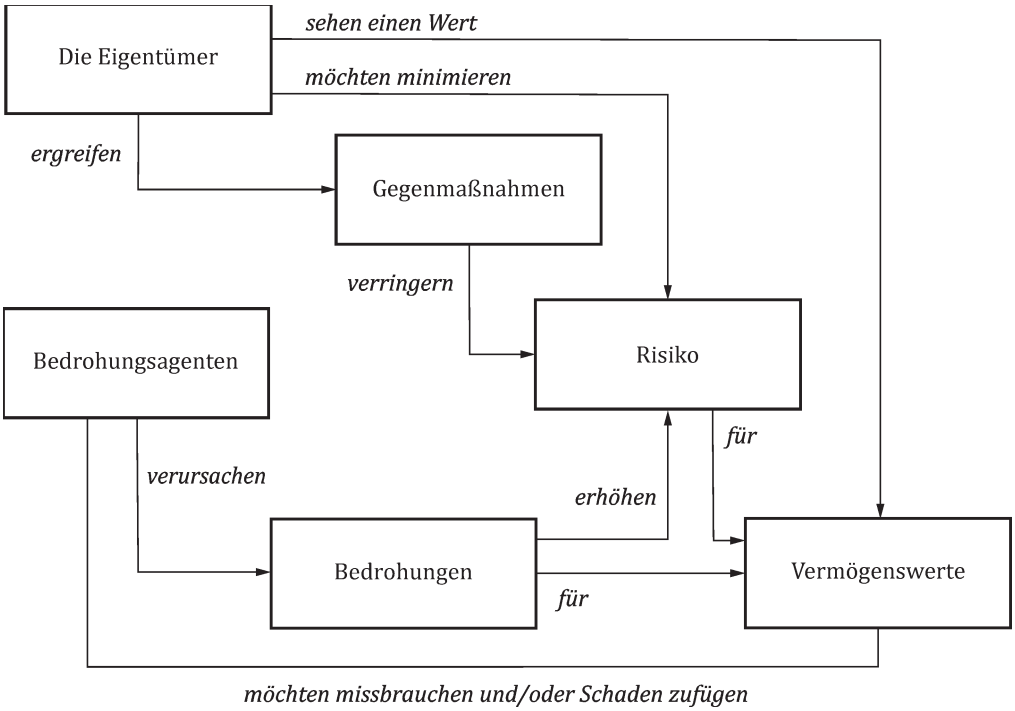

Bild 1 — Sicherheitskonzepte und Beziehungen

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.

BEISPIEL 2 Beispiele für Bedrohungsagenten umfassen Hacker, böswillige Benutzer, nicht-böswillige Benutzer (die manchmal Fehler machen), Computerprozesse und Unfälle.

Die Eigentümer der Vermögenswerte können diese Bedrohungen als potentielle Quelle für eine Schädigung der Vermögenswerte wahrnehmen, was zu einer Minderung ihres Werts führt. 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 Maßnahmen ergriffen, um die Risiken auf die Vermögenswerte zu reduzieren. Diese Maßnahmen können aus IT-bezogenen Maßnahmen (z. B. Firewalls und Chipkarten) und Nicht-IT-Maßnahmen (z. B. Wachleute und Verfahren) bestehen. Siehe auch ISO/IEC 27001 und ISO/IEC 27002 für eine allgemeinere Erörterung zu Sicherheitsmaßnahmen und deren Implementierung und Verwaltung.

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 Maßnahmen sind angemessen: wenn die angewandten Maßnahmen das tun, was sie versprechen, sind die Bedrohungen für die Vermögenswerte abgewehrt;

— die Maßnahmen sind korrekt: wenn die angewandten Maßnahmen das tun, was sie versprechen.

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-1:2024-01

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

Bild 2 beschreibt die in diesem Abschnitt erörterten Evaluierungskonzepte und Beziehungen.

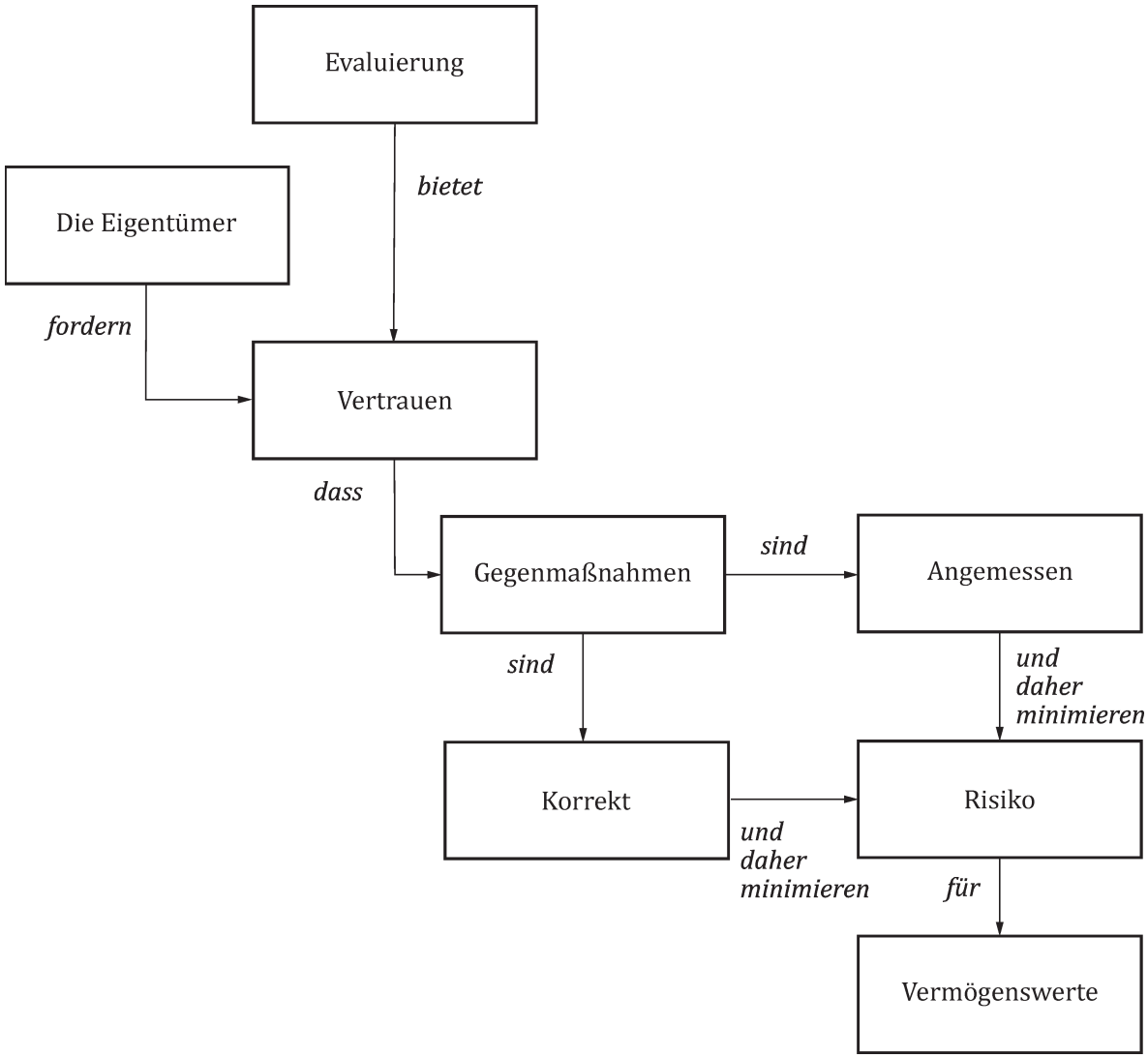

Bild 2 — Evaluierungskonzepte und Beziehungen

Die Angemessenheit der Sicherheitsmaßnahmen wird bei einer Evaluierung über ein Konstrukt namens Sicherheitsvorgabe (ST) analysiert.

6.3 Kernkonstrukte des Paradigmas der Normenreihe ISO/IEC 15408

6.3.1 Allgemein

Die Normenreihe ISO/IEC 15408 legt ein flexibles Rahmenwerk für die Evaluierung von IT-Produkten fest.

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-1:2024-01

Um Verbrauchergruppen und technischen Gemeinschaften die Möglichkeit zu geben, ihre Sicherheitsbedürfnisse auszudrücken, und um das Verfassen geeigneter Dokumente zu erleichtern, die diese Bedürfnisse zum Ausdruck bringen, sind im Paradigma fünf Konstrukte vorgesehen: Paket, PP, PP-Modul, PP-Konfiguration und ST.

Da eine Evaluierung unterschiedliche Vertrauenswürdigkeitsanforderungen der Verbraucher (Risikoeigentümer) erfüllen muss, stellt die Normenreihe ISO/IEC 15408 verschiedene Werkzeuge zur Verfügung, darunter wohlgeformte Vertrauenswürdigkeitskomponenten (ISO/IEC 15408-3) sowie einen Mechanismus zur Definition erweiterter Vertrauenswürdigkeitskomponenten (ISO/IEC 15408-1).

Benutzer der Normenreihe ISO/IEC 15408 können auch aus vordefinierten Paketen wählen, einschließlich der Pakete für die EAL (basierend auf ISO/IEC 15408-5), oder aus einem Rahmen für die Definition von Evaluierungsmethoden und -aufgaben (ISO/IEC 15408-4) und der zugehörigen Evaluierungsmethodologie (basierend auf ISO/IEC 18045).

6.3.2 Konformitätstypen

Drei verschiedene Typen der Konformität mit PP und PP-Konfigurationen wurden definiert, um den Bedürfnissen der Verbraucher (Risikoeigentümer) gerecht zu werden. Es handelt sich um genaue, strikte und nachweisliche Konformität. Sie werden ausführlich in Anhang E beschrieben.

Die PP, PP-Module und PP-Konfigurationen müssen einen Konformitätstyp festlegen.

Die ST beanspruchen Konformität mit den PP und PP-Konfigurationen nach deren Konformitätstypen. Die PP können auch Konformität mit anderen PP nach ihrem Konformitätstyp beanspruchen.

Konformitätstypen, Konformitätsansprüche und Beziehungen zwischen Konformitätstypen der PP, PP-Module und PP-Konfigurationen werden in Anhang E beschrieben und müssen in Verbindung mit den Abschnitten des vorliegenden Dokuments verwendet werden.

6.3.3 Weitergabe von Sicherheitsanforderungen

6.3.3.1 Pakete

Pakete beschreiben eine Reihe zusammenhängender Sicherheitsanforderungen, die häufig gemeinsam verwendet werden. Pakete sind oft so gestaltet, dass sie wiederverwendet werden können, was eine gewisse Vergleichbarkeit zwischen den PP, PP-Modulen und ST, die sie verwenden, ermöglicht.

Sicherheitsfunktionspakete können zur Festlegung von Sicherheitsprotokollen oder anderen Sicherheitsfunktionskonzepten verwendet werden.

Vertrauenswürdigkeitspakete können verwendet werden, um die Bedingungen und Prozesse wie Spezifikation, Design, Entwicklung, Prüfung und Auslieferung festzulegen, auf deren Grundlage der TOE entwickelt und konfiguriert wird.

Kernanforderungen für Pakete können Abschnitt 9 entnommen werden. Anhang A enthält zusätzliche Informationen und Anforderungen an Pakete, die in Verbindung mit den Abschnitten dieses Dokuments verwendet werden müssen.

ISO/IEC 15408-3 enthält Evaluationskriterien und spezifische Anforderungen für zu evaluierende ST, PP und PP-Module, die Pakete verwenden können, und ISO/IEC 15408-5 enthält einige vordefinierte Vertrauenswürdigkeitspakete, die von Autoren für PP, PP-Module, PP-Konfigurationen und ST verwendet werden können.

6.3.3.2 Schutzprofile (PP)

Die PP beschreiben einen TOE-Typ und die Vertrauenswürdigkeitsanforderungen (SAR) und die Sicherheitsfunktionsanforderungen (SFR), die für diesen Typ von TOE vorgesehen sind.

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-1:2024-01

Die auf anderen PP beruhenden PP können zur weiteren Präzisierung eines TOE-Typs verwendet werden.

Die PP können entweder einen Standard- oder einen direkten Begründungsansatz verfolgen.

Kernanforderungen an ein PP können Abschnitt 10 entnommen werden und weitere Informationen finden sich in Anhang B, der in Verbindung mit den Abschnitten dieses Dokuments verwendet werden muss.

ISO/IEC 15408-3 enthält Evaluierungskriterien für die PP.

6.3.3.3 PP-Module und PP-Konfigurationen

PP-Konfigurationen bauen auf den Konzepten der PP und PP-Module auf.

Ein PP-Modul kann verwendet werden, um den generischen TOE-Typ eines Basis-PP zu präzisieren oder um Sicherheitsanforderungen für bestimmte Technologien hinzuzufügen, die optional mit dem in den Basis-PP definierten TOE-Typ verbunden sein können. PP-Module können auch auf anderen PP-Modulen beruhen. Darüber hinaus bestehen PP-Konfigurationen aus einem TOE-Typ und einem Satz von Anforderungen, die in mehreren PP und möglicherweise PP-Modulen festgelegt sind (dies sind die Komponenten der PP-Konfiguration).

Dieses Konzept wird in Abschnitt 11 und Anhang C ausführlicher beschrieben.

BEISPIEL Ein PP-Modul beschreibt die SFR für die Bluetooth-Technologie. Ein weiteres PP-Modul beschreibt die SFR für Wireless-LAN-Clients. Unter Verwendung einer PP-Konfiguration können die SFR für jede dieser Technologien mit einem PP kombiniert werden, das einen TOE-Typ beschreibt, z. B. ein PP für ein Betriebssystem oder ein PP für ein Mobilgerät. In diesem Zusammenhang wird das PP, das den TOE-Typ beschreibt, als Basis-PP bezeichnet. Eine PP-Konfiguration beschreibt, welche PP und PP-Module kombiniert werden, um eine Spezifikation zu erstellen, die alle in den entsprechenden PP und PP-Modulen genannten Anforderungen enthält.

In diesem Beispiel wäre es möglich, sechs PP-Konfigurationen festzulegen:

a) Betriebssystem mit Bluetooth;

b) Betriebssystem in Verbindung mit einem Wireless Client;

c) Betriebssystem mit Bluetooth und Wireless Client;

d) Mobilgerät mit Bluetooth;

e) Mobilgerät mit einem Wireless Client;

f) Mobilgerät mit Bluetooth und Wireless Client.

6.3.3.4 Sicherheitsvorgaben (ST)

6.3.3.4.1 Allgemein

Der Abschnitt stellt eine vereinfachte Sicht des ST-Konstrukts dar. Eine ausführlichere und vollständige Beschreibung des ST-Konzepts und der inhaltlichen Anforderungen kann 11.3.3 und Anhang D entnommen werden, die in Verbindung mit den Abschnitten dieses Dokuments verwendet werden müssen.

ISO/IEC 15408-3 enthält Evaluationskriterien und spezifische Anforderungen für zu evaluierende ST.

6.3.3.4.2 Zweck einer ST

Die ST ist ein Schlüsseldokument, das mit der Festlegung der Sicherheitsproblemdefinition (SPD) für den TOE beginnt. Dazu gehört die Festlegung der zu schützenden Vermögenswerte und deren Bedrohungen. Die ST berücksichtigt dann alle relevanten Annahmen und beschreibt die Sicherheitsmaßnahmen, die eingerichtet

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-1:2024-01

werden müssen, um nachzuweisen, dass diese Bedrohungen abgewehrt werden. Wenn die Sicherheitsmaßnahmen das tun, was sie versprechen, sind die Bedrohungen abgewehrt.

Zu den beiden Gruppen von Sicherheitsmaßnahmen gehören:

a) die Sicherheitszielsetzungen für den TOE: diese beschreiben die Sicherheitsmaßnahme(n), für die in der Evaluierung Korrektheit bestimmt wird;

b) die Sicherheitszielsetzungen für die Betriebsumgebung: diese beschreiben die Sicherheitsmaßnahmen, für die in der Evaluierung Korrektheit nicht bestimmt wird.

Die Gründe für diese Einteilung sind wie folgt.

— Die Normenreihe ISO/IEC 15408 eignet sich für die Bewertung der Korrektheit von IT-Entwicklungs- und Produktionsumgebungen sowie des Produktlebenszyklusmanagements. Die von der Betriebsumgebung geforderten Sicherheitsmaßnahmen sind nicht Gegenstand der Evaluierung nach der Normenreihe ISO/IEC 15408.

— Die Bewertung der Korrektheit von Sicherheitsmaßnahmen kostet Zeit und Geld und die Bewertung aller Sicherheitsmaßnahmen ist daher vermutlich unzumutbar.

— Die Korrektheit einiger Sicherheitsmaßnahmen kann auch bereits in einer anderen Evaluierung bewertet worden sein. Daher ist es nicht wirtschaftlich, diese Korrektheit erneut zu bewerten.

In der ST werden die Sicherheitszielsetzungen für den TOE durch die Festlegung der SFR weiter ausgeführt. Diese SFRs müssen in einer standardisierten Sprache formuliert sein (beschrieben in ISO/IEC 15408-2), um Genauigkeit sicherzustellen und Vergleichbarkeit herzustellen.

Zusammengefasst zeigen die ST Folgendes:

— die SFRs erfüllen die Sicherheitszielsetzungen für den TOE;

— die Sicherheitszielsetzungen für den TOE und die Sicherheitszielsetzungen für die Betriebsumgebung behandeln die SPD und wehren insbesondere die Bedrohungen ab;

— und deshalb behandeln die SFRs und die Sicherheitszielsetzungen für die Betriebsumgebung die SPD und wehren insbesondere die Bedrohungen ab.

Daraus folgt, dass ein korrekter TOE, d. h. ein TOE, der die SFRs in Verbindung mit einer korrekten Betriebsumgebung erfüllt, die wiederum die Sicherheitszielsetzungen für diese Betriebsumgebung erfüllt, die Bedrohungen abwehren wird. Die Korrektheit des TOEs und die Korrektheit der Betriebsumgebung werden in 6.3.3.4.3 und 6.3.3.4.4 separat erörtert.

In einigen Fällen ist es angemessen, eine ST zu definieren, die die Sicherheitszielsetzungen für den TOE weglässt und die SFR direkt dem SPD zuordnet. Dies ist eine ST „mit direkter Begründung“ und wird in 11.3.3 und Anhang D ausführlich erläutert.

Eine ST kann als eigenständiges Dokument für einen bestimmten TOE definiert werden oder sie kann mit einer bereits vorhandenen PP-Konfiguration bzw. einem oder mehreren bereits vorhandenen PP konform sein. Diese Dokumente ermöglichen es, generische Definitionen eines TOE-Typs vorzunehmen, die eine Vergleichbarkeit der Evaluierungsergebnisse zwischen den TOE sowie die Erzielung von Effizienzgewinnen ermöglichen.

Pakete, PP, PP-Module und PP-Konfigurationen, die zur Spezifikation einer ST beitragen können, werden in 6.3.3.1, 6.3.3.2 und 6.3.3.3 vorgestellt.

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-1:2024-01

6.3.3.4.3 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 in der Lage sein, die Vermögenswerte zu beschädigen und/oder zu missbrauchen.

Diese Schwachstellen können z. B. durch schlechtes Design, versehentliche Fehler während der Entwicklung, absichtliches Hinzufügen von Schadcode oder schlechtes Konfigurationsmanagement entstehen.

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

— Prüfen des TOEs;

— Untersuchen unterschiedlicher Design-Darstellungen des TOEs;

— Untersuchen der physischen Sicherheit der Entwicklungsumgebung des TOEs.

Die ST bietet eine strukturierte Beschreibung dieser Tätigkeiten zur Bestimmung der Korrektheit in Form von SAR. Diese SAR müssen in einer standardisierten Sprache formuliert sein (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.

6.3.3.4.4 Korrektheit der Betriebsumgebung

Auch eine Betriebsumgebung kann inkorrekt festgelegt 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 Normenreihe ISO/IEC 15408 ist allerdings keine Zusicherung zur Korrektheit der Betriebsumgebung möglich, d. h. die Betriebsumgebung wird nicht evaluiert.

In Bezug auf die Evaluierung wird davon ausgegangen, dass die Betriebsumgebung eine 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 anzuwenden.

BEISPIEL 1 Wenn für ein Betriebssystem-TOE die Sicherheitszielsetzungen für die Betriebsumgebung besagen „Die Betriebsumgebung stellt sicher, dass Entitäten aus einem nicht vertrauenswürdigen Netzwerk nur per FTP- auf den TOE zugreifen können“, so kann der Verbraucher eine evaluierte Firewall auswählen und so konfigurieren, dass nur FTP-Zugriff auf den TOE zu erlaubt ist.

BEISPIEL 2 Wenn die Sicherheitszielsetzungen für die Betriebsumgebung besagen: „Die Betriebsumgebung muss sicherstellen, dass alle Administratoren sich nicht böswillig verhalten“, so kann der Verbraucher seine Verträge mit den Administratoren um entsprechende Strafsanktionen erweitern, aber diese Bestimmung ist nicht Teil einer Evaluierung, die sich auf die Normenreihe ISO/IEC 15408 stützt.

ANMERKUNG Das Internet ist ein Beispiel für ein nicht vertrauenswürdiges Netzwerk.

6.3.4 Erfüllung der Bedürfnisse der Verbraucher (Risikoeigentümer)

6.3.4.1 Allgemein

Die Verbraucher (Risikoeigentümer) können unterschiedliche Ansätze verfolgen, um sich zu vergewissern, dass die von ihnen verwendeten Produkte die SPD abdecken. 6.3.4.2 und 6.3.4.3 stellen diese Ansätze vor.

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-1:2024-01

Darüber hinaus bietet ISO/IEC 15408-4 Verfahren zur Definition spezifischer Evaluierungsaufgaben für die Vertrauenswürdigkeitsanforderungen.

6.3.4.2 Evaluierung mit Einfach-Vertrauenswürdigkeit

Die Evaluierung mit Einfach-Vertrauenswürdigkeit ist die Art von Evaluierung, die in früheren Revisionen der Normenreihe ISO/IEC 15408 festgelegt wurde. Bei einer Evaluierung mit Einfach-Vertrauenswürdigkeit wird eine einzige Menge an SAR auf den gesamten TOE angewandt.

Das Paradigma der Evaluierung mit Einfach-Vertrauenswürdigkeit:

— setzt voraus, dass der gesamte TOE denselben SAR unterliegt;

— wird verwendet, wenn ein einziger Satz an SAR den Sicherheitsanforderungen für den TOE angemessen ist.

Eine Evaluierung mit Einfach-Vertrauenswürdigkeit basiert auf einer ST, die Konformität mit den PP oder einer PP-Konfiguration beanspruchen kann, aber darauf angewiesen ist, dass alle beanspruchten PP oder PP-Konfigurationskomponenten identische Sätze oder übergeordnete Sätze von Vertrauenswürdigkeitskomponenten spezifizieren. Eine Evaluierung auf der Grundlage einer ST, die keinen Anspruch auf Konformität mit PP oder einer PP-Konfiguration erhebt, ist demnach eine Evaluierung mit Einfach-Vertrauenswürdigkeit.

6.3.4.3 Evaluierung mit Mehrfach-Vertrauenswürdigkeit

Das Paradigma der Evaluierung mit Mehrfach-Vertrauenswürdigkeit besteht in der Anwendung verschiedener Vertrauenswürdigkeitsanforderungen auf verschiedene Teile der TSF (Teil-TSF), während eine Gesamtmenge an SAR für den gesamten TOE durchgesetzt wird.

Das Paradigma der Evaluierung mit Mehrfach-Vertrauenswürdigkeit:

— richtet sich an heterogene IT-Produkte, bei denen unterschiedliche Sicherheitsbedürfnisse im Rahmen einer Evaluierung mit Einfach-Vertrauenswürdigkeit eine unterschiedliche Vertrauenswürdigkeit erfordern;

— stellt sicher, dass die Anforderungen mit Mehrfach-Vertrauenswürdigkeit den Sicherheitsbedürfnissen für das IT-Produkt gerecht werden.

Technisch gesehen wird eine Evaluierung mit Mehrfach-Vertrauenswürdigkeit durch eine ST gesteuert, die mit einer (und nur einer) PP-Konfiguration mit Mehrfach-Vertrauenswürdigkeit übereinstimmt. Die PP-Konfiguration mit Mehrfach-Vertrauenswürdigkeit stellt sicher, dass die Anwendung unterschiedlicher Vertrauenswürdigkeitsanforderungen auf verschiedene Teile der TSF mit deren Sicherheitsbedürfnissen widerspruchsfrei ist. Bei diesem Evaluierungsansatz erzwingt jede Teil-TSF eine bestimmte Sicherheitsfunktionalität, z. B. ein Authentifizierungsprotokoll, eine Firewall-Richtlinie, den Boot-Prozess oder Verschlüsselungs-/Entschlüsselungsoperationen; in einigen Fällen kann die Teil-TSF mit einer Teilmenge von TOE-Komponenten verbunden sein, z. B. einem TPM, einer kryptographischen Bibliothek oder einem Kartenleser.

Das Paradigma mit Mehrfach-Vertrauenswürdigkeit ist vor allem in den folgenden Situationen von Bedeutung:

— ein Produkt, bei dem einige Sicherheitsfunktionen eine höhere Vertrauenswürdigkeit erfordern als die übrigen, z. B. eine Schlüsselspeicher- und -verarbeitungseinheit, ein sicheres Systemstartmodul;

— ein Produkt, bei dem einige Teile der Sicherheitsfunktionalität nicht die gleiche hohe Vertrauenswürdigkeit bei der Evaluierung erfordern wie andere, stärker exponierte Teile, z. B. ein Internet-Gateway mit Unterstützung für Personal-Area-Network-Protokolle;

— eine Produktfamilie, bei der einige Sicherheitsfunktionen von allen Produkten mit der gleichen Vertrauenswürdigkeit gemeinsam benutzt und einige Sicherheitsfunktionen für verschiedene Anwendungsfälle auf

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-1:2024-01

unterschiedliche Weise implementiert werden, z. B. in einem manipulationssicheren Modul oder in einem Softwaremodul oder durch COTS, was eine andere Vertrauenswürdigkeit erfordert;

Ein Beispiel dafür ist eine Familie von biometrischen Authentifizierungsgeräten, die entweder eine Übereinstimmung auf dem Gerät oder auf dem Server oder beides aufweisen. Dies kann zu einem PP für das Authentifizierungsgerät ohne die Abgleichsfunktion und zu zwei PP-Modulen für die verschiedenen Arten von Abgleichsfunktionen führen, die jeweils einen eigenen Satz von Vertrauenswürdigkeitsanforderungen haben. Für das Gerät können drei PP-Konfigurationen festgelegt werden: PP mit jedem der PP-Module, PP mit beiden PP-Modulen. Eine ähnliche Situation ergibt sich beispielsweise für eine Familie mobiler Anwendungen, die entweder eine durch White-Box-Techniken gesicherte Software-Kryptobibliothek oder eine hardwarebasierte Kryptobibliothek verwenden, oder für eine Familie von Zahlungsterminals mit IC- und/oder Magnetkartenlesern.

Mehrfach-Vertrauenswürdigkeit ist auch für Produkte relevant, die Konformität mit verschiedenen PP mit unterschiedlichen Vertrauenswürdigkeitspaketen beanspruchen: Durch die Definition und Evaluierung einer PP-Konfiguration ermöglicht das Paradigma mit Mehrfach-Vertrauenswürdigkeit bessere Kontrolle über mögliche Inkonsistenzen zwischen diesen PP. Die Evaluierung von elektronischen Reisepässen, bei denen sowohl eine einfache als auch eine erweiterte Zugangssteuerung implementiert ist, stellt ein typisches Beispiel dar, da diese Zugangskontrollmechanismen unterschiedlichen Sicherheitsproblemen und Vertrauenswürdigkeitsanforderungen unterliegen.

7 Festlegung von Sicherheitsanforderungen

7.1 Sicherheitsproblemdefinition (SPD)

7.1.1 Allgemein

Die SPD definiert das zu behandelnde Sicherheitsproblem und kann in den PP, PP-Modulen und den ST erscheinen. Die SPD ist, was die Normenreihe ISO/IEC 15408 betrifft, axiomatisch, d. h. der Prozess der Ableitung der SPD fällt nicht in den Anwendungsbereich der Normenreihe ISO/IEC 15408.

SPD-Elemente können Konfigurationen oder Anforderungen zugeordnet werden, die für den gegebenen TOE-Typ optional sind, z. B. in einem Fall, in dem der TOE verteilt ist oder in dem optionale funktionale Anforderungen (wie in 7.3.2.6 beschrieben) festgelegt sind. Dies ist zulässig, solange der fakultative Charakter der SPD-Elemente (und alle damit verbundenen Zielsetzungen und funktionalen Anforderungen) wie in diesem Dokument beschrieben angegeben wird.

ANMERKUNG 1 Der Nutzen der Ergebnisse einer Evaluierung hängt stark von der Qualität der SPD ab. Daher ist es häufig den Aufwand wert, die entsprechenden Ressourcen aufzuwenden und klar definierte Prozesse und Analysen zu verwenden, um eine gute SPD herzuleiten. ISO/IEC 15446 enthält Leitlinien für die Ableitung einer SPD.

ANMERKUNG 2 Nach ISO/IEC 15408-3 ist es nicht verpflichtend, in allen Abschnitten Aussagen zu treffen. Ein PP mit Bedrohungen erfordert keine OSP und umgekehrt. Ein PP kann außerdem Annahmen weglassen.

ANMERKUNG 3 Bei einem physisch verteilten TOE ist es vorzuziehen, die relevanten Bedrohungen, OSPs und Annahmen separat für die einzelnen Domänen der TOE-Betriebsumgebung zu behandeln.

7.1.2 Bedrohungen

Die SPD beschreibt die vom TOE, seiner Betriebsumgebung oder einer Kombination dieser beiden zu begegnenden Bedrohungen.

Eine Bedrohung besteht aus einer unerwünschten Aktion, die von einem Bedrohungsagenten gegen einen Vermögenswert durchgeführt wird.

Nachteilige Aktionen beeinflussen eine oder mehrere Eigenschaften eines Vermögenswerts, aus dem dieser Vermögenswert seinen Wert ableitet.

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-1:2024-01

Bedrohungsagenten können als individuelle Entitäten beschrieben werden, aber in einigen Fällen ist es vorzuziehen, sie z. B. als Typen von Entitäten, Gruppen von Entitäten zu beschreiben.

BEISPIEL 1 Beispiele für Bedrohungsagenten sind:

— Hacker;

— Benutzer;

— Computerprozesse;

— Unfälle.

Bedrohungsagenten können noch weiter über Attribute wie Fachkenntnis, Ressourcen, Möglichkeiten und Motivation beschrieben werden.

BEISPIEL 2 Beispiele für Bedrohungen sind:

— ein Hacker (mit beträchtlicher Fachkenntnis, Standardausrüstung und Bezahlung für seine Tätigkeit), der aus der Ferne vertrauliche Dateien aus einem Unternehmensnetzwerk kopiert;

— ein Wurm, der die Leistung eines WANs erheblich verringert;

— ein Systemadministrator, der die Privatsphäre eines Benutzers verletzt;

— jemand, der im Internet vertrauliche elektronische Kommunikation abhört.

7.1.3 Organisatorische Sicherheitsrichtlinien (OSP)

Die SPD beschreibt die OSPs, die vom TOE, seiner Betriebsumgebung oder einer Kombination aus beidem durchgesetzt werden sollen.

OSPs sind in der Betriebsumgebung auferlegte Sicherheitsregeln, Verfahren oder Leitlinien. OSPs können von einer Organisation zum Steuern der Betriebsumgebung eines TOEs oder von Gesetzgebungsorganen oder Aufsichtsbehörden erstellt werden. OSPs können für den TOE und/oder die Betriebsumgebung des TOEs gelten.

BEISPIEL Beispiele für OSPs sind:

— „Alle von der Regierung verwendeten Produkte müssen mit der nationalen Norm für Passworterzeugung und Passwortverschlüsselung konform sein“;

— „Nur Benutzer mit Systemadministratorrechten und Freigabe durch die Sicherheitsabteilung dürfen den Dateiserver der Abteilung verwalten“.

7.1.4 Annahmen

Die SPD beschreibt die für die Betriebsumgebung gemachten Annahmen, um die Sicherheitsfunktionalität bereitzustellen. Wenn der TOE in einer Betriebsumgebung eingesetzt wird, die diese Annahmen nicht erfüllt, besteht die Möglichkeit, dass der TOE nicht mehr seine vollständige Sicherheitsfunktionalität bereitstellen kann. Annahmen können sich auf physische Eigenschaften, Personal und Konnektivität der Betriebsumgebung beziehen.

BEISPIEL Beispiele für Annahmen sind:

— Annahmen über den Nicht-TOE-Teil des Produkts;

  — es wird angenommen, dass der TOE in ein Gerät integriert wird, das eine hardwarebasierte Vertrauensbasis bietet.

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-1:2024-01

— Annahmen zu physischen Aspekten der Betriebsumgebung;

  — es wird angenommen, dass der TOE in einem Raum eingesetzt wird, der zur Minimierung von elektromagnetischen Emanationen ausgelegt ist;

  — es wird angenommen, dass die Administratorkonsolen des TOEs in einem Bereich mit Zugangsbeschränkung eingesetzt werden.

— Annahmen zu Personalaspekten der Betriebsumgebung;

  — es wird angenommen, dass Benutzer des TOEs ausreichend in der Bedienung des TOEs geschult werden;

  — es wird angenommen, dass Benutzer des TOEs eine Freigabe für als nationales Geheimnis eingestufte Informationen haben;

  — es wird angenommen, dass Benutzer des TOEs ihre Passwörter nicht aufschreiben.

— Annahmen zu Aspekten der Konnektivität der Betriebsumgebung;

  — es wird angenommen, dass eine Arbeitsstation mit mindestens 10 GB freiem Speicherplatz für den Betrieb des TOEs verfügbar ist;

  — es wird angenommen, dass der TOE die einzige Anwendung auf der Arbeitsstation ist, die kein Betriebssystem ist;

  — es wird angenommen, dass der TOE nicht mit einem nicht vertrauenswürdigen Netzwerk verbunden wird.

ANMERKUNG Diese Annahmen werden zum Zeitpunkt der Evaluierung als wahr betrachtet, sie werden in keiner Weise überprüft. Daher können Annahmen nur in Bezug zur Betriebsumgebung getroffen werden. Annahmen können niemals in Bezug auf das Verhalten des TOEs gemacht werden, weil eine Evaluierung aus der Bewertung der gemachten Aussagen über den TOE besteht und nicht aus der Annahme, dass diese Aussagen über den TOE wahr sind. Dennoch helfen die ST-, PP- und PP-Konfigurationsevaluierungen dabei, unrealistische Annahmen für den TOE-Typ und die Betriebsumgebung aufzudecken, die unannehmbar werden können.

7.2 Sicherheitszielsetzungen

7.2.1 Allgemein

Sicherheitszielsetzungen sind eine präzise Aussage zur angestrebten Lösung des Sicherheitsproblems. Die Rolle der Sicherheitszielsetzungen umfasst drei Aspekte:

a) Bereitstellung einer allgemeinen Lösung des Problems in natürlicher Sprache. Die Sicherheitszielsetzungen bestehen aus einem Satz an Aussagen ohne übermäßig viele Einzelheiten und bilden gemeinsam die allgemeine Lösung für das Sicherheitsproblem. Die Abstraktionsebene der Sicherheitszielsetzungen zielt auf Klarheit und Verständlichkeit für sachkundige potentielle Verbraucher des TOEs. Die Sicherheitszielsetzungen sind in natürlicher Sprache formuliert;

b) Einteilung dieser Lösung in zwei Teillösungen, die die Rollen des TOE und seiner Betriebsumgebung widerspiegeln, um jeweils einen Teil des Problems anzusprechen. Eine wie in einer Sicherheitszielsetzung beschriebene allgemeine Sicherheitslösung in einer ST ist in zwei Teillösungen unterteilt. Diese Teillösungen werden Sicherheitszielsetzungen für den TOE und Sicherheitszielsetzung für die Betriebsumgebung genannt;

c) Darstellung dieser Teillösungen als Gesamtlösung des Problems.

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-1:2024-01