DIN EN ISO/IEC 18045:2021-02 (D)

Informationstechnik - Sicherheitstechniken - Methodik für die Bewertung der IT-Sicherheit (ISO/IEC 18045:2008); Deutsche Fassung EN ISO/IEC 18045:2020, nur auf CD-ROM

Inhalt

Seite

Europäisches Vorwort 7
Vorwort 8
Rechtliche Hinweise 9
Einleitung 10
1 Anwendungsbereich 11
2 Normative Verweisungen 11
3 Begriffe 11
4 Symbole und Abkürzungen 13
5 Überblick 13
5.1 Gliederung dieser Internationalen Norm 13
6 Typographische Konventionen 14
6.1 Terminologie 14
6.2 Verbgebrauch 14
6.3 Allgemeine Evaluierungsleitlinien 14
6.4 Beziehung zwischen den Strukturen von ISO/IEC 15408 und ISO/IEC 18045 14
7 Evaluierungsprozess und damit verbundene Arbeitsaufgaben 15
7.1 Einleitung 15
7.2 Überblick über den Evaluierungsprozess 16
7.2.1 Zielsetzungen 16
7.2.2 Verantwortlichkeiten der Rollen 16
7.2.3 Beziehung der Rollen 16
7.2.4 Allgemeines Evaluierungsmodell 16
7.2.5 Evaluatoren-Entscheidungen 17
7.3 Eingabearbeitsaufgabe der Evaluierung 19
7.3.1 Zielsetzungen 19
7.3.2 Anwendungshinweise 19
7.3.3 Management der Teilarbeitsaufgabe der Evaluationsnachweise 20
7.4 Evaluierungsunteraufgaben 20
7.5 Ausgabearbeitsaufgabe der Evaluierung 20
7.5.1 Zielsetzungen 20
7.5.2 Management der Evaluierungsausgaben 21
7.5.3 Anwendungshinweise 21
7.5.4 OR-Teilarbeitsaufgabe schreiben 21
7.5.5 ETR-Teilarbeitsaufgabe schreiben 22
8 Klasse APE: Evaluierung des Schutzprofils 27
8.1 Einleitung 27
8.2 Anwendungshinweise 28
8.2.1 Wiederverwendung der Evaluierungsergebnisse von zertifizierten PPs 28
8.3 PP-Einleitung (APE_INT) 28
8.3.1 Evaluierung der Unteraufgabe (APE_INT.1) 28
8.4 Konformitätsansprüche (APE_CCL) 30
8.4.1 Evaluierung der Unteraufgabe (APE_CCL.1) 30

8.5 Sicherheitsproblemdefinition (APE_SPD) 37
8.5.1 Evaluierung der Unteraufgabe (APE_SPD.1) 37
8.6 Sicherheitszielsetzungen (APE_OBJ) 38
8.6.1 Evaluierung der Unteraufgabe (APE_OBJ.1) 38
8.6.2 Evaluierung der Unteraufgabe (APE_OBJ.2) 39
8.7 Erweiterte Komponentendefinition (APE_ECD) 41
8.7.1 Evaluierung der Unteraufgabe (APE_ECD.1) 41
8.8 Sicherheitsanforderungen (APE_REQ) 45
8.8.1 Evaluierung der Unteraufgabe (APE_REQ.1) 45
8.8.2 Evaluierung der Unteraufgabe (APE_REQ.2) 49

9 Klasse ASE: Evaluierung der Sicherheitsvorgabe 54
9.1 Einleitung 54
9.2 Anwendungshinweise 54
9.2.1 Wiederverwendung der Evaluierungsergebnisse von zertifizierten PPs 54
9.3 ST-Einleitung (ASE_INT) 54
9.3.1 Evaluierung der Unteraufgabe (ASE_INT.1) 54
9.4 Konformitätsansprüche (ASE_CCL) 57
9.4.1 Evaluierung der Unteraufgabe (ASE_CCL.1) 57
9.5 Sicherheitsproblemdefinition (ASE_SPD) 66
9.5.1 Evaluierung der Unteraufgabe (ASE_SPD.1) 66
9.6 Sicherheitszielsetzungen (ASE_OBJ) 67
9.6.1 Evaluierung der Unteraufgabe (ASE_OBJ.1) 67
9.6.2 Evaluierung der Unteraufgabe (ASE_OBJ.2) 68
9.7 Erweiterte Komponentendefinition (ASE_ECD) 70
9.7.1 Evaluierung der Unteraufgabe (ASE_ECD.1) 70
9.8 Sicherheitsanforderungen (ASE_REQ) 74
9.8.1 Evaluierung der Unteraufgabe (ASE_REQ.1) 74
9.8.2 Evaluierung der Unteraufgabe (ASE_REQ.2) 78
9.9 Zusammenfassende Spezifikation des TOEs (ASE_TSS) 83
9.9.1 Evaluierung der Unteraufgabe (ASE_TSS.1) 83
9.9.2 Evaluierung der Unteraufgabe (ASE_TSS.2) 83

10 Klasse ADV: Entwicklung 85
10.1 Einleitung 85
10.2 Anwendungshinweise 85
10.3 Sicherheitsarchitektur (ADV_ARC) 86
10.3.1 Evaluierung der Unteraufgabe (ADV_ARC.1) 86
10.4 Funktionsspezifikation (ADV_FSP) 91
10.4.1 Evaluierung der Unteraufgabe (ADV_FSP.1) 91
10.4.2 Evaluierung der Unteraufgabe (ADV_FSP.2) 94
10.4.3 Evaluierung der Unteraufgabe (ADV_FSP.3) 100
10.4.4 Evaluierung der Unteraufgabe (ADV_FSP.4) 105
10.4.5 Evaluierung der Unteraufgabe (ADV_FSP.5) 111
10.4.6 Evaluierung der Unteraufgabe (ADV_FSP.6) 118
10.5 Darstellung der Implementierung (ADV_IMP) 118
10.5.1 Evaluierung der Unteraufgabe (ADV_IMP.1) 118
10.5.2 Evaluierung der Unteraufgabe (ADV_IMP.2) 120
10.6 TSF-Interna (ADV_INT) 120
10.6.1 Evaluierung der Unteraufgabe (ADV_INT.1) 120
10.6.2 Evaluierung der Unteraufgabe (ADV_INT.2) 123
10.6.3 Evaluierung der Unteraufgabe (ADV_INT.3) 125
10.7 Modellierung der Sicherheitspolitik (ADV_SPM) 125
10.7.1 Evaluierung der Unteraufgabe (ADV_SPM.1) 125
10.8 TOE-Design (ADV_TDS) 125
10.8.1 Evaluierung der Unteraufgabe (ADV_TDS.1) 125
10.8.2 Evaluierung der Unteraufgabe (ADV_TDS.2) 129
10.8.3 Evaluierung der Unteraufgabe (ADV_TDS.3) 134
10.8.4 Evaluierung der Unteraufgabe (ADV_TDS.4) 144

10.8.5 Evaluierung der Unteraufgabe (ADV_TDS.5) ... 155
10.8.6 Evaluierung der Unteraufgabe (ADV_TDS.6) ... 155

11 Klasse AGD: Leitliniendokumente ... 155
11.1 Einleitung ... 155
11.2 Anwendungshinweise ... 155
11.3 Operative Leitlinien für Benutzer (AGD_OPE) ... 155
11.3.1 Evaluierung der Unteraufgabe (AGD_OPE.1) ... 155
11.4 Vorbereitende Verfahren (AGD_PRE) ... 158
11.4.1 Evaluierung der Unteraufgabe (AGD_PRE.1) ... 158

12 Klasse ALC: Unterstützung des Lebenszyklus ... 160
12.1 Einleitung ... 160
12.2 CM-Funktionen (ALC_CMC) ... 161
12.2.1 Evaluierung der Unteraufgabe (ALC_CMC.1) ... 161
12.2.2 Evaluierung der Unteraufgabe (ALC_CMC.2) ... 162
12.2.3 Evaluierung der Unteraufgabe (ALC_CMC.3) ... 164
12.2.4 Evaluierung der Unteraufgabe (ALC_CMC.4) ... 168
12.2.5 Evaluierung der Unteraufgabe (ALC_CMC.5) ... 174
12.3 CM-Umfang (ALC_CMS) ... 181
12.3.1 Evaluierung der Unteraufgabe (ALC_CMS.1) ... 181
12.3.2 Evaluierung der Unteraufgabe (ALC_CMS.2) ... 182
12.3.3 Evaluierung der Unteraufgabe (ALC_CMS.3) ... 183
12.3.4 Evaluierung der Unteraufgabe (ALC_CMS.4) ... 184
12.3.5 Evaluierung der Unteraufgabe (ALC_CMS.5) ... 185
12.4 Lieferung (ALC_DEL) ... 186
12.4.1 Evaluierung der Unteraufgabe (ALC_DEL.1) ... 186
12.5 Entwicklungssicherheit (ALC_DVS) ... 188
12.5.1 Evaluierung der Unteraufgabe (ALC_DVS.1) ... 188
12.5.2 Evaluierung der Unteraufgabe (ALC_DVS.2) ... 190
12.6 Mängelbeseitigung (ALC_FLR) ... 194
12.6.1 Evaluierung der Unteraufgabe (ALC_FLR.1) ... 194
12.6.2 Evaluierung der Unteraufgabe (ALC_FLR.2) ... 196
12.6.3 Evaluierung der Unteraufgabe (ALC_FLR.3) ... 200
12.7 Definition des Lebenszyklus (ALC_LCD) ... 206
12.7.1 Evaluierung der Unteraufgabe (ALC_LCD.1) ... 206
12.7.2 Evaluierung der Unteraufgabe (ALC_LCD.2) ... 207
12.8 Tools und Techniken (ALC_TAT) ... 209
12.8.1 Evaluierung der Unteraufgabe (ALC_TAT.1) ... 209
12.8.2 Evaluierung der Unteraufgabe (ALC_TAT.2) ... 211
12.8.3 Evaluierung der Unteraufgabe (ALC_TAT.3) ... 213

13 Klasse ATE: Prüfungen ... 216
13.1 Einleitung ... 216
13.2 Anwendungshinweise ... 216
13.2.1 Verständnis des erwarteten Verhaltens des TOEs ... 217
13.2.2 Prüfen gegenüber alternativen Ansätzen zur Überprüfung des erwarteten Verhaltens der Funktionalität ... 218
13.2.3 Überprüfung der Angemessenheit der Prüfungen ... 218
13.3 Abdeckung (ATE_COV) ... 219
13.3.1 Evaluierung der Unteraufgabe (ATE_COV.1) ... 219
13.3.2 Evaluierung der Unteraufgabe (ATE_COV.2) ... 219
13.3.3 Evaluierung der Unteraufgabe (ATE_COV.3) ... 221
13.4 Tiefe (ATE_DPT) ... 221
13.4.1 Evaluierung der Unteraufgabe (ATE_DPT.1) ... 221
13.4.2 Evaluierung der Unteraufgabe (ATE_DPT.2) ... 223
13.4.3 Evaluierung der Unteraufgabe (ATE_DPT.3) ... 226
13.4.4 Evaluierung der Unteraufgabe (ATE_DPT.4) ... 229
13.5 Funktionsprüfungen (ATE_FUN) ... 229
13.5.1 Evaluierung der Unteraufgabe (ATE_FUN.1) ... 229

13.5.2 Evaluierung der Unteraufgabe (ATE_FUN.2) ... 232
13.6 Unabhängiges Prüfen (ATE_IND) ... 232
13.6.1 Evaluierung der Unteraufgabe (ATE_IND.1) ... 232
13.6.2 Evaluierung der Unteraufgabe (ATE_IND.2) ... 237
13.6.3 Evaluierung der Unteraufgabe (ATE_IND.3) ... 242

14 Klasse AVA: Anfälligkeitsbewertung ... 242
14.1 Einleitung ... 242
14.2 Anfälligkeitsanalyse (AVA_VAN) ... 243
14.2.1 Evaluierung der Unteraufgabe (AVA_VAN.1) ... 243
14.2.2 Evaluierung der Unteraufgabe (AVA_VAN.2) ... 248
14.2.3 Evaluierung der Unteraufgabe (AVA_VAN.3) ... 255
14.2.4 Evaluierung der Unteraufgabe (AVA_VAN.4) ... 264
14.2.5 Evaluierung der Unteraufgabe (AVA_VAN.5) ... 272

15 Klasse ACO: Zusammensetzung ... 273
15.1 Einleitung ... 273
15.2 Anwendungshinweise ... 273
15.3 Begründung der Zusammensetzung (ACO_COR) ... 274
15.3.1 Evaluierung der Unteraufgabe (ACO_COR.1) ... 274
15.4 Entwicklungsnachweis (ACO_DEV) ... 281
15.4.1 Evaluierung der Unteraufgabe (ACO_DEV.1) ... 281
15.4.2 Evaluierung der Unteraufgabe (ACO_DEV.2) ... 282
15.4.3 Evaluierung der Unteraufgabe (ACO_DEV.3) ... 284
15.5 Verlässlichkeit der abhängigen Komponente (ACO_REL) ... 287
15.5.1 Evaluierung der Unteraufgabe (ACO_REL.1) ... 287
15.5.2 Evaluierung der Unteraufgabe (ACO_REL.2) ... 289
15.6 Prüfen des zusammengesetzten TOEs (ACO_CTT) ... 292
15.6.1 Evaluierung der Unteraufgabe (ACO_CTT.1) ... 292
15.6.2 Evaluierung der Unteraufgabe (ACO_CTT.2) ... 295
15.7 Anfälligkeitsanalyse der Zusammensetzung (ACO_VUL) ... 298
15.7.1 Evaluierung der Unteraufgabe (ACO_VUL.1) ... 298
15.7.2 Evaluierung der Unteraufgabe (ACO_VUL.2) ... 301
15.7.3 Evaluierung der Unteraufgabe (ACO_VUL.3) ... 305

Anhang A (informativ) Allgemeine Evaluierungsleitlinien ... 310
A.1 Zielsetzungen ... 310
A.2 Probenahme ... 310
A.3 Abhängigkeiten ... 312
A.3.1 Abhängigkeiten zwischen Aufgaben ... 312
A.3.2 Abhängigkeiten zwischen Unteraufgaben ... 312
A.3.3 Abhängigkeiten zwischen Aktionen ... 313
A.4 Standortbesichtigungen ... 313
A.4.1 Einleitung ... 313
A.4.2 Allgemeiner Ansatz ... 314
A.4.3 Orientierungshilfe für die Erstellung der Checkliste ... 314
A.4.4 Beispiel für eine Checkliste ... 316
A.5 Zuständigkeiten des Schemas ... 318

Anhang B (informativ) Anfälligkeitsbewertung (AVA) ... 320
B.1 Was ist eine Anfälligkeitsanalyse? ... 320
B.2 Erstellung einer Anfälligkeitsanalyse durch den Evaluator ... 321
B.2.1 Generische Leitlinien für Anfälligkeiten ... 321
B.2.2 Identifizierung potentieller Anfälligkeiten ... 329
B.3 Wenn das Angriffspotential genutzt wird ... 332
B.3.1 Entwickler ... 332
B.3.2 Evaluator ... 332
B.4 Berechnung des Angriffspotentials ... 334
B.4.1 Anwendung des Angriffspotentials ... 334
B.4.2 Charakterisierung des Angriffspotentials ... 335
B.5 Beispielrechnung für direkten Angriff ... 341