

E DIN EN ISO/IEC 18045:2020-06 (D/E)

Erscheinungsdatum: 2020-05-22

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

Information technology - Security techniques - Methodology for IT security evaluation (ISO/IEC 18045:2008); German and English version prEN ISO/IEC 18045:2020, only on 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.....	28
8.1 Einleitung.....	28

8.2	Anwendungshinweise.....	29
8.2.1	Wiederverwendung der Evaluierungsergebnisse von zertifizierten PPs.....	29
8.3	PP-Einleitung (APE_INT)	29
8.3.1	Evaluierung der Unteraufgabe (APE_INT.1)	29
8.4	Konformitätsansprüche (APE_CCL)	31
8.4.1	Evaluierung der Unteraufgabe (APE_CCL.1)	31
8.5	Sicherheitsproblemdefinition (APE_SPD)	38
8.5.1	Evaluierung der Unteraufgabe (APE_SPD.1)	38
8.6	Sicherheitszielsetzungen (APE_OBJ)	39
8.6.1	Evaluierung der Unteraufgabe (APE_OBJ.1)	39
8.6.2	Evaluierung der Unteraufgabe (APE_OBJ.2)	40
8.7	Erweiterte Komponentendefinition (APE_ECD)	43
8.7.1	Evaluierung der Unteraufgabe (APE_ECD.1)	43
8.8	Sicherheitsanforderungen (APE_REQ)	47
8.8.1	Evaluierung der Unteraufgabe (APE_REQ.1)	47
8.8.2	Evaluierung der Unteraufgabe (APE_REQ.2)	50
9	Klasse ASE: Evaluierung der Sicherheitsvorgabe	55
9.1	Einleitung.....	55
9.2	Anwendungshinweise.....	56
9.2.1	Wiederverwendung der Evaluierungsergebnisse von zertifizierten PPs.....	56
9.3	ST-Einleitung (ASE_INT).....	56
9.3.1	Evaluierung der Unteraufgabe (ASE_INT.1).....	56
9.4	Konformitätsansprüche (ASE_CCL)	59
9.4.1	Evaluierung der Unteraufgabe (ASE_CCL.1)	59
9.5	Sicherheitsproblemdefinition (ASE_SPD)	68
9.5.1	Evaluierung der Unteraufgabe (ASE_SPD.1)	68
9.6	Sicherheitszielsetzungen (ASE_OBJ)	70
9.6.1	Evaluierung der Unteraufgabe (ASE_OBJ.1).....	70
9.6.2	Evaluierung der Unteraufgabe (ASE_OBJ.2).....	70
9.7	Erweiterte Komponentendefinition (ASE_ECD)	73
9.7.1	Evaluierung der Unteraufgabe (ASE_ECD.1).....	73
9.8	Sicherheitsanforderungen (ASE_REQ).....	77
9.8.1	Evaluierung der Unteraufgabe (ASE_REQ.1)	77
9.8.2	Evaluierung der Unteraufgabe (ASE_REQ.2)	80
9.9	Zusammenfassende Spezifikation des TOEs (ASE_TSS)	85
9.9.1	Evaluierung der Unteraufgabe (ASE_TSS.1).....	85
9.9.2	Evaluierung der Unteraufgabe (ASE_TSS.2).....	86
10	Klasse ADV: Entwicklung.....	87
10.1	Einleitung.....	87
10.2	Anwendungshinweise.....	88
10.3	Sicherheitsarchitektur (ADV_ARC).....	88
10.3.1	Evaluierung der Unteraufgabe (ADV_ARC.1).....	88
10.4	Funktionsspezifikation (ADV_FSP).....	94
10.4.1	Evaluierung der Unteraufgabe (ADV_FSP.1).....	94
10.4.2	Evaluierung der Unteraufgabe (ADV_FSP.2).....	97
10.4.3	Evaluierung der Unteraufgabe (ADV_FSP.3).....	103
10.4.4	Evaluierung der Unteraufgabe (ADV_FSP.4).....	108
10.4.5	Evaluierung der Unteraufgabe (ADV_FSP.5).....	114
10.4.6	Evaluierung der Unteraufgabe (ADV_FSP.6).....	121
10.5	Darstellung der Implementierung (ADV_IMP)	121
10.5.1	Evaluierung der Unteraufgabe (ADV_IMP.1).....	121
10.5.2	Evaluierung der Unteraufgabe (ADV_IMP.2).....	123
10.6	TSF-Interna (ADV_INT)	123
10.6.1	Evaluierung der Unteraufgabe (ADV_INT.1).....	123
10.6.2	Evaluierung der Unteraufgabe (ADV_INT.2).....	126
10.6.3	Evaluierung der Unteraufgabe (ADV_INT.3).....	128
10.7	Modellierung der Sicherheitspolitik (ADV_SPM).....	128

10.7.1	Evaluierung der Unteraufgabe (ADV_SPM.1)	128
10.8	TOE-Design (ADV_TDS)	128
10.8.1	Evaluierung der Unteraufgabe (ADV_TDS.1)	128
10.8.2	Evaluierung der Unteraufgabe (ADV_TDS.2)	132
10.8.3	Evaluierung der Unteraufgabe (ADV_TDS.3)	138
10.8.4	Evaluierung der Unteraufgabe (ADV_TDS.4)	147
10.8.5	Evaluierung der Unteraufgabe (ADV_TDS.5)	158
10.8.6	Evaluierung der Unteraufgabe (ADV_TDS.6)	158
11	Klasse AGD: Leitliniendokumente	158
11.1	Einleitung	158
11.2	Anwendungshinweise	158
11.3	Operative Leitlinien für Benutzer (AGD_OPE)	158
11.3.1	Evaluierung der Unteraufgabe (AGD_OPE.1)	158
11.4	Vorbereitende Verfahren (AGD_PRE)	162
11.4.1	Evaluierung der Unteraufgabe (AGD_PRE.1)	162
12	Klasse ALC: Unterstützung des Lebenszyklus	164
12.1	Einleitung	164
12.2	CM-Funktionen (ALC_CMC)	164
12.2.1	Evaluierung der Unteraufgabe (ALC_CMC.1)	164
12.2.2	Evaluierung der Unteraufgabe (ALC_CMC.2)	166
12.2.3	Evaluierung der Unteraufgabe (ALC_CMC.3)	167
12.2.4	Evaluierung der Unteraufgabe (ALC_CMC.4)	172
12.2.5	Evaluierung der Unteraufgabe (ALC_CMC.5)	177
12.3	CM-Umfang (ALC_CMS)	185
12.3.1	Evaluierung der Unteraufgabe (ALC_CMS.1)	185
12.3.2	Evaluierung der Unteraufgabe (ALC_CMS.2)	185
12.3.3	Evaluierung der Unteraufgabe (ALC_CMS.3)	186
12.3.4	Evaluierung der Unteraufgabe (ALC_CMS.4)	187
12.3.5	Evaluierung der Unteraufgabe (ALC_CMS.5)	189
12.4	Lieferung (ALC_DEL)	190
12.4.1	Evaluierung der Unteraufgabe (ALC_DEL.1)	190
12.5	Entwicklungssicherheit (ALC_DVS)	192
12.5.1	Evaluierung der Unteraufgabe (ALC_DVS.1)	192
12.5.2	Evaluierung der Unteraufgabe (ALC_DVS.2)	194
12.6	Mängelbeseitigung (ALC_FLR)	198
12.6.1	Evaluierung der Unteraufgabe (ALC_FLR.1)	198
12.6.2	Evaluierung der Unteraufgabe (ALC_FLR.2)	200
12.6.3	Evaluierung der Unteraufgabe (ALC_FLR.3)	204
12.7	Definition des Lebenszyklus (ALC_LCD)	210
12.7.1	Evaluierung der Unteraufgabe (ALC_LCD.1)	210
12.7.2	Evaluierung der Unteraufgabe (ALC_LCD.2)	211
12.8	Tools und Techniken (ALC_TAT)	213
12.8.1	Evaluierung der Unteraufgabe (ALC_TAT.1)	213
12.8.2	Evaluierung der Unteraufgabe (ALC_TAT.2)	215
12.8.3	Evaluierung der Unteraufgabe (ALC_TAT.3)	218
13	Klasse ATE: Prüfungen	220
13.1	Einleitung	220
13.2	Anwendungshinweise	221
13.2.1	Verständnis des erwarteten Verhaltens des TOEs	221
13.2.2	Prüfen gegenüber alternativen Ansätzen zur Überprüfung des erwarteten Verhaltens der Funktionalität	222
13.2.3	Überprüfung der Angemessenheit der Prüfungen	222
13.3	Abdeckung (ATE_COV)	223
13.3.1	Evaluierung der Unteraufgabe (ATE_COV.1)	223
13.3.2	Evaluierung der Unteraufgabe (ATE_COV.2)	223
13.3.3	Evaluierung der Unteraufgabe (ATE_COV.3)	225

13.4	Tiefe (ATE_DPT).....	225
13.4.1	Evaluierung der Unteraufgabe (ATE_DPT.1).....	225
13.4.2	Evaluierung der Unteraufgabe (ATE_DPT.2).....	227
13.4.3	Evaluierung der Unteraufgabe (ATE_DPT.3).....	230
13.4.4	Evaluierung der Unteraufgabe (ATE_DPT.4).....	233
13.5	Funktionsprüfungen (ATE_FUN)	233
13.5.1	Evaluierung der Unteraufgabe (ATE_FUN.1).....	233
13.5.2	Evaluierung der Unteraufgabe (ATE_FUN.2).....	236
13.6	Unabhängiges Prüfen (ATE_IND).....	236
13.6.1	Evaluierung der Unteraufgabe (ATE_IND.1).....	236
13.6.2	Evaluierung der Unteraufgabe (ATE_IND.2).....	241
13.6.3	Evaluierung der Unteraufgabe (ATE_IND.3).....	246
14	Klasse AVA: Anfälligkeitsbewertung.....	247
14.1	Einleitung.....	247
14.2	Anfälligkeitsanalyse (AVA_VAN)	247
14.2.1	Evaluierung der Unteraufgabe (AVA_VAN.1)	247
14.2.2	Evaluierung der Unteraufgabe (AVA_VAN.2)	252
14.2.3	Evaluierung der Unteraufgabe (AVA_VAN.3)	260
14.2.4	Evaluierung der Unteraufgabe (AVA_VAN.4)	269
14.2.5	Evaluierung der Unteraufgabe (AVA_VAN.5)	277
15	Klasse ACO: Zusammensetzung.....	277
15.1	Einleitung.....	277
15.2	Anwendungshinweise.....	277
15.3	Begründung der Zusammensetzung (ACO_COR).....	278
15.3.1	Evaluierung der Unteraufgabe (ACO_COR.1).....	278
15.4	Entwicklungsnachweis (ACO_DEV).....	285
15.4.1	Evaluierung der Unteraufgabe (ACO_DEV.1).....	285
15.4.2	Evaluierung der Unteraufgabe (ACO_DEV.2).....	286
15.4.3	Evaluierung der Unteraufgabe (ACO_DEV.3).....	288
15.5	Verlässlichkeit der abhängigen Komponente (ACO_REL).....	291
15.5.1	Evaluierung der Unteraufgabe (ACO_REL.1)	291
15.5.2	Evaluierung der Unteraufgabe (ACO_REL.2)	293
15.6	Prüfen des zusammengesetzten TOEs (ACO_CTT).....	296
15.6.1	Evaluierung der Unteraufgabe (ACO_CTT.1).....	296
15.6.2	Evaluierung der Unteraufgabe (ACO_CTT.2)	299
15.7	Anfälligkeitsanalyse der Zusammensetzung (ACO_VUL)	303
15.7.1	Evaluierung der Unteraufgabe (ACO_VUL.1).....	303
15.7.2	Evaluierung der Unteraufgabe (ACO_VUL.2).....	306
15.7.3	Evaluierung der Unteraufgabe (ACO_VUL.3).....	310
Anhang A (informativ) Allgemeine Evaluierungsleitlinien.....		315
A.1	Zielsetzungen.....	315
A.2	Probenahme.....	315
A.3	Abhängigkeiten.....	317
A.3.1	Abhängigkeiten zwischen Aufgaben	317
A.3.2	Abhängigkeiten zwischen Unteraufgaben	317
A.3.3	Abhängigkeiten zwischen Aktionen.....	318
A.4	Standortbesichtigungen.....	318
A.4.1	Einleitung.....	318
A.4.2	Allgemeiner Ansatz.....	319
A.4.3	Orientierungshilfe für die Erstellung der Checkliste	319
A.4.4	Beispiel für eine Checkliste.....	321
A.5	Zuständigkeiten des Schemas	323
Anhang B (informativ) Anfälligkeitsbewertung (AVA).....		325
B.1	Was ist eine Anfälligkeitsanalyse?.....	325
B.2	Erstellung einer Anfälligkeitsanalyse durch den Evaluator.....	326
B.2.1	Generische Leitlinien für Anfälligkeiten.....	326

B.2.2	Identifizierung potentieller Anfälligkeiten.....	334
B.3	Wenn das Angriffspotential genutzt wird	338
B.3.1	Entwickler.....	338
B.3.2	Evaluator	338
B.4	Berechnung des Angriffspotentials	339
B.4.1	Anwendung des Angriffspotentials	339
B.4.2	Charakterisierung des Angriffspotentials.....	340
B.5	Beispielrechnung für direkten Angriff.....	347