DIN EN 18031-2:2025-03 (D)

Gemeinsame Sicherheitsanforderungen für Funkanlagen - Teil 2: Funkanlagen, die Daten verarbeiten, insbesondere internetfähige Funkanlagen, Kinderbetreuungsfunkanlagen, Spielzeugfunkanlagen und tragbare Funkanlagen; Deutsche Fassung EN 18031-2:2024

Inhalt

Seite

Europäisches Vorwort ... 9
Einleitung ... 10
1 Anwendungsbereich ... 11
2 Normative Verweisungen ... 11
3 Begriffe ... 11
4 Abkürzungen ... 17
5 Anwendbarkeit dieses Dokuments ... 18
6 Anforderungen ... 22
6.1 [ACM] Zugangssteuerungsmechanismus (en: Access Control Mechanism) ... 22
6.1.1 [ACM-1] Anwendbarkeit von Zugangssteuerungsmechanismen ... 22
6.1.2 [ACM-2] Entsprechende Zugangssteuerungsmechanismen ... 27
6.1.3 [ACM-3] Standardmäßige Zugangssteuerung für Kinder bei Spielzeugen ... 32
6.1.4 [ACM-4] Standard-Zugangssteuerung zu Datenschutzwerten von Kindern für Spielzeuge und Kinderbetreuungsgeräte ... 37
6.1.5 [ACM-5] Zugangssteuerung durch Eltern/Erziehungsberechtigte für Kinder bei Spielzeugen ... 43
6.1.6 [ACM-6] Zugangssteuerung durch Eltern/Erziehungsberechtigte für den Zugang anderer Entitäten auf die verwalteten Datenschutzwerte von Kindern bei Spielzeugen ... 48
6.2 [AUM] Authentisierungsmechanismus (en: Authentication Mechanism) ... 53
6.2.1 [AUM-1] Anwendbarkeit von Authentisierungsmechanismen ... 53
6.2.2 [AUM-2] Angemessene Authentisierungsmechanismen ... 63
6.2.3 [AUM-3] Authentifikator-Validierung ... 70
6.2.4 [AUM-4] Änderung von Authentifikatoren ... 74
6.2.5 [AUM-5] Passwortstärke ... 78
6.2.6 [AUM-6] Schutz vor Brute-Force-Angriffen ... 85
6.3 [SUM] Sicherer Aktualisierungsmechanismus (en: Secure Update Mechanism) ... 89
6.3.1 [SUM-1] Anwendbarkeit von Aktualisierungsmechanismen ... 89
6.3.2 [SUM-2] Sichere Aktualisierungen ... 93
6.3.3 [SUM-3] Automatisierte Aktualisierungen ... 98
6.4 [SSM] Sicherer Speichermechanismus (en: Secure Storage Mechanism) ... 102
6.4.1 [SSM-1] Anwendbarkeit von sicheren Speichermechanismen ... 102
6.4.2 [SSM-2] Angemessener Integritätsschutz für sichere Speichermechanismen ... 107
6.4.3 [SSM-3] Angemessener Vertraulichkeitsschutz für sichere Speichermechanismen ... 112
6.5 [SCM] Sicherer Kommunikationsmechanismus (en: Secure Communication Mechanism) ... 118
6.5.1 [SCM-1] Anwendbarkeit von sicheren Kommunikationsmechanismen ... 118
6.5.2 [SCM-2] Angemessener Integritäts- und Authentizitätsschutz für sichere Kommunikationsmechanismen ... 124
6.5.3 [SCM-3] Angemessener Vertraulichkeitsschutz für sichere Kommunikationsmechanismen ... 131
6.5.4 [SCM-4] Angemessener Replay-Schutz für sichere Kommunikationsmechanismen ... 136
6.6 [LGM] Protokollierungsmechanismus (en: Logging Mechanism) ... 142
6.6.1 [LGM-1] Anwendbarkeit von Protokollierungsmechanismen ... 142

6.6.2 [LGM-2] Dauerhafte Speicherung von Protokolldaten ... 145
6.6.3 [LGM-3] Mindestanzahl an dauerhaft gespeicherten Ereignissen ... 148
6.6.4 [LGM-4] Zeitbezogene Informationen der dauerhaft gespeicherten Protokolldaten ... 151
6.7 [DLM] Löschungsmechanismus (en: Deletion Mechanism) ... 155
6.7.1 [DLM-1] Anwendbarkeit von Löschungsmechanismen ... 155
6.8 [UNM] Benutzer-Benachrichtigungsmechanismus (en: User Notification Mechanism) ... 160
6.8.1 [UNM-1] Anwendbarkeit von Benutzer-Benachrichtigungsmechanismen ... 160
6.8.2 [UNM-2] Angemessener Inhalt der Benutzerbenachrichtigung ... 164
6.9 [CCK] Vertrauliche kryptographische Schlüssel (en: Confidential Cryptographic Keys) ... 167
6.9.1 [CCK-1] Angemessene CCKs ... 167
6.9.2 [CCK-2] Mechanismen zur Erzeugung des CCK ... 171
6.9.3 [CCK-3] Verhinderung von statischen Vorgabewerten für vorinstallierte CCKs ... 176
6.10 [GEC] Allgemeine Gerätefähigkeiten (en: General Equipment Capabilities) ... 180
6.10.1 [GEC-1] Aktuelle Software und Hardware ohne öffentlich bekannte ausnutzbare Schwachstellen ... 180
6.10.2 [GEC-2] Begrenzung der Offenlegung von Diensten über entsprechende Netzwerkschnittstellen ... 185
6.10.3 [GEC-3] Konfiguration von optionalen Diensten und zugehörigen offengelegten Netzwerkschnittstellen ... 189
6.10.4 [GEC-4] Dokumentation von zugänglichen Netzwerkschnittstellen und über Netzwerkschnittstellen zugänglichen Diensten ... 193
6.10.5 [GEC-5] Keine unnötigen externen Schnittstellen ... 196
6.10.6 [GEC-6] Eingabevalidierung ... 199
6.10.7 [GEC-7] Dokumentation externer Sensorikfähigkeiten ... 203
6.11 [CRY] Kryptographie (en: Cryptography) ... 207
6.11.1 [CRY-1] Bewährte Verfahrensweisen für Kryptographie ... 207

Anhang A (informativ) Begründung ... 213
A.1 Allgemeines ... 213
A.2 Begründung ... 213
A.2.1 Normenfamilie ... 213
A.2.2 Sicherheit durch Gestaltung (en: Security by Design) ... 213
A.2.3 Bedrohungsmodellierung und Sicherheitsrisikobeurteilung ... 214
A.2.4 Beurteilung der funktionalen Suffizienz ... 215
A.2.5 Umsetzungskategorien ... 216
A.2.6 Werte ... 216
A.2.7 Mechanismen ... 218
A.2.8 Beurteilungskriterien ... 219
A.2.9 Schnittstellen ... 221

Anhang B (informativ) Abbildung mit EN IEC 62443-4-2:2019 ... 224
B.1 Allgemeines ... 224
B.2 Abbildung ... 224

Anhang C (informativ) Abbildung mit ETSI EN 303 645 (Cyber Security for Consumer Internet of Things: Baseline Requirements) ... 227
C.1 Allgemeines ... 227
C.2 Abbildung ... 227

Anhang D (informativ) Abbildung mit Sicherheitsbewertungsstandard für IoT-Plattformen (SESIP, en: Security Evaluation for Secure IoT Platforms) ... 232
D.1 Allgemeines ... 232
D.2 Abbildung ... 232

Anhang ZA (informativ) Zusammenhang zwischen dieser Europäischen Norm und der Delegierten Verordnung (EU) 2022/30 zur Ergänzung der Verordnung 2014/53/EU des Europäischen Parlaments und des Rates im Hinblick auf die Anwendung der grundlegenden Anforderungen, wie in Artikel 3(3), Punkt (d), Punkt (e) und Punkt (f) dieser abzudeckenden Verordnung in Bezug genommen ... 235

Literaturhinweise ... 236

Bilder

Bild 1 — Entscheidungsbaum für Anforderung ACM-1 ... 25

Bild 2 — Entscheidungsbaum für Anforderung ACM-2 ... 30

Bild 3 — Entscheidungsbaum für Anforderung ACM-3 ... 34

Bild 4 — Entscheidungsbaum für Anforderung ACM-4 ... 40

Bild 5 — Entscheidungsbaum für Anforderung ACM-5 ... 45

Bild 6 — Entscheidungsbaum für Anforderung ACM-6 ... 50

Bild 7 — Entscheidungsbaum für Anforderung AUM-1-1 ... 57

Bild 8 — Entscheidungsbaum für Anforderung AUM-1-2 ... 61

Bild 9 — Entscheidungsbaum für Anforderung AUM-2-1 ... 66

Bild 10 — Entscheidungsbaum für Anforderung AUM-2-2 ... 69

Bild 11 — Entscheidungsbaum für Anforderung AUM-3 ... 72

Bild 12 — Entscheidungsbaum für Anforderung AUM-4 ... 76

Bild 13 — Entscheidungsbaum für Anforderung AUM-5-1 ... 80

Bild 14 — Entscheidungsbaum für Anforderung AUM-5-2 ... 83

Bild 15 — Entscheidungsbaum für Anforderung AUM-6 ... 87

Bild 16 — Entscheidungsbaum für Anforderung SUM-1 ... 92

Bild 17 — Entscheidungsbaum für Anforderung SUM-2 ... 96

Bild 18 — Entscheidungsbaum für Anforderung SUM-3 ... 100

Bild 19 — Entscheidungsbaum für Anforderung SSM-1 ... 105

Bild 20 — Entscheidungsbaum für Anforderung SSM-2 ... 110

Bild 21 — Entscheidungsbaum für Anforderung SSM-3 ... 115

Bild 22 — Entscheidungsbaum für Anforderung SCM-1 ... 122

Bild 23 — Entscheidungsbaum für Anforderung SCM-2 ... 128

Bild 24 — Entscheidungsbaum für Anforderung SCM-3 ... 134

Bild 25 — Entscheidungsbaum für Anforderung SCM-4 ... 140

Bild 26 — Entscheidungsbaum für Anforderung LGM-1 ... 144

Bild 27 — Entscheidungsbaum für Anforderung LGM-2 ... 147

Bild 28 — Entscheidungsbaum für Anforderung LGM-3 150

Bild 29 — Entscheidungsbaum für Anforderung LGM-4 153

Bild 30 — Entscheidungsbaum für Anforderung DLM-1 158

Bild 31 — Entscheidungsbaum für Anforderung UNM-1 162

Bild 32 — Entscheidungsbaum für Anforderung UNM-2 165

Bild 33 — Entscheidungsbaum für Anforderung CCK-1 169

Bild 34 — Entscheidungsbaum für Anforderung CCK-2 174

Bild 35 — Entscheidungsbaum für Anforderung CCK-3 178

Bild 36 — Entscheidungsbaum für Anforderung GEC-1 183

Bild 37 — Entscheidungsbaum für Anforderung GEC-2 187

Bild 38 — Entscheidungsbaum für Anforderung GEC-3 190

Bild 39 — Entscheidungsbaum für Anforderung GEC-4 194

Bild 40 — Entscheidungsbaum für Anforderung GEC-5 197

Bild 41 — Entscheidungsbaum für Anforderung GEC-6 201

Bild 42 — Entscheidungsbaum für Anforderung GEC-7 205

Bild 43 — Entscheidungsbaum für Anforderung CRY-1 210

Bild A.1 — Datenschutzwert der Anlage 217

Bild A.2 — Sicherheitswert der Anlage 218

Bild A.3 — Beispiel für einen Entscheidungsbaum 219

Bild A.4 — Beispiel: Nachweis durch Entscheidungsbaum 221

Bild A.5 — Beispiel: Laptop mit einer eingebauten Tastatur 222

Bild A.6 — Beispiel: Gerät mit einer USB-Tastatur 222

Bild A.7 — Beispiel: Benutzungsschnittstelle über dem Netzwerk 222

Bild A.8 — Beispiel: USB-Drucker 223

Bild A.9 — Beispiel: Netzwerkdrucker 223

Tabellen

Tabelle 1 — Struktur der Anforderungen 19

Tabelle A.1 — STRIDE 214

Tabelle A.2 — Sicherheitsanforderungen, Fähigkeiten, Eindämmungstechniken und Gestaltungsgrundsätze 215

Tabelle A.3 — Werte und grundlegende Anforderungen 216

Tabelle A.4 — Schnittstellen 221

Tabelle ZA.1 — Zusammenhang zwischen dieser Europäischen Norm und der Richtlinie 2014/53/EU [Amtsblatt L 153] 235