DIN EN 17927:2024-03 (D)

Sicherheitsbewertungsstandard für IoT-Plattformen (SESIP) - Ein effektives Verfahren zur Anwendung der Cybersicherheitsbewertung und Wiederverwendung für vernetzte Produkte; Deutsche Fassung EN 17927:2023

Inhalt

Seite

Europäisches Vorwort 6

Einleitung 7

1 Anwendungsbereich 8

2 Normative Verweisungen 8

3 Begriffe 8

4 Überblick 9
4.1 Allgemeines 9
4.2 SESIP Konzepte 10
4.3 IoT Anwendungsfälle und Bedrohungsmodell 10
4.3.1 Allgemeines 10
4.3.2 Architektur 11
4.3.3 Vermögenswerte 11
4.3.4 Angreifer und Bedrohungen 12
4.4 Lebenszyklus eines vernetzten Produkts 13
4.5 Wiederverwendbarkeit beim SESIP 14
4.5.1 Allgemeines 14
4.5.2 Aufbau vernetzter Produkte aus vernetzten Plattformen 15
4.5.3 Additivzusammensetzung im Rahmen von SESIP 17
4.6 Zugänglichkeit und Transparenz 21
4.7 Selbstbewertung der Sicherheit in SESIP 21
4.8 Katalog der Sicherheitsfunktionen und Vertrauenswürdigkeitspakete 22
4.9 SESIP Profile und -Zuordnungen 23
4.9.1 Allgemeines 23
4.9.2 SESIP Profile 23
4.9.3 SESIP Zuordnungen 23

5 Sicherheitsfunktionsanforderungen (SFR) 24
5.1 Allgemeines 24
5.2 Identifizierung und Attestierung von Plattformen und Anwendungen 24
5.2.1 Allgemeines 24
5.2.2 Verifizierung der Plattformidentität 25
5.2.3 Verifizierung der Identität der Plattforminstanz 25
5.2.4 Attestierung der Echtheit der Plattform 25
5.2.5 Sichere Initialisierung der Plattform 26
5.2.6 Attestierung des Zustands der Plattform 26
5.2.7 Attestierung der Echtheit der Anwendung 27
5.2.8 Attestierung des Zustands der Anwendung 27
5.3 Produktlebenszyklus: Zurücksetzen auf Werkseinstellungen/Installieren/Aktualisieren/Außerbetriebnahme 27
5.3.1 Allgemeines 27
5.3.2 Zurücksetzen der Plattform auf die Werkseinstellungen 28
5.3.3 Sichere Installation der Anwendung 28
5.3.4 Sichere Aktualisierung der Plattform 29
5.3.5 Sichere Aktualisierung der Anwendung 29

5.3.6 Sichere Deinstallation der Anwendung 30
5.3.7 Außerbetriebnahme der Plattform 30
5.3.8 Rückgabe der Plattform in der Praxis 31
5.4 Sichere Kommunikation 31
5.4.1 Allgemeines 31
5.4.2 Unterstützung für eine sichere Kommunikation 31
5.4.3 Durchsetzung einer sicheren Kommunikation 32
5.5 Zusätzliche Angreiferabwehr 33
5.5.1 Allgemeines 33
5.5.2 Begrenzte Abwehr von physischen Angreifern 33
5.5.3 Physische Angreiferabwehr 34
5.5.4 Software-Angriffsabwehr: Isolierung der Plattform 34
5.5.5 Software-Angriffsabwehr: Isolierung von Plattformteilen 35
5.5.6 Software-Angriffsabwehr: Isolierung von Anwendungsteilen 35
5.6 Kryptographische Funktionalität 36
5.6.1 Allgemeines 36
5.6.2 Kryptographische Operation 36
5.6.3 Generierung kryptographischer Schlüssel 37
5.6.4 Kryptographischer KeyStore (Schlüsselspeicher) 37
5.6.5 Kyptographische Generierung von Zufallszahlen 38
5.7 Konformitätsfunktionen 38
5.7.1 Allgemeines 38
5.7.2 Sichere vertrauenswürdige Speicherung 39
5.7.3 Sichere vertrauliche Speicherung 39
5.7.4 Sichere verschlüsselte Speicherung 39
5.7.5 Sichere Datenserialisierung 40
5.7.6 Bereinigung von Restinformationen 41
5.7.7 Erstellung und Speicherung von Auditprotokollen 41
5.7.8 Zuverlässiger Index 42
5.7.9 Sicheres Debugging 42
5.7.10 Sichere Wiederherstellung 43
5.7.11 Sicheres Backup und Wiederherstellung 43
5.7.12 Allgemeines Sicherheitsmerkmal der Plattform 43
5.8 Zugriffskontrolle 44
5.8.1 Allgemeines 44
5.8.2 Privilegierte Zugriffskontrolle 44
5.8.3 Authentifizierte Zugriffskontrolle 44
5.9 Verfügbarkeit 45
5.9.1 Allgemeines 45
5.9.2 Eingeschränkte Anforderungen an die Umgebungsfähigkeit 45
5.9.3 Unterstützung der Verfügbarkeit 45
5.10 Mindestsatz an Sicherheitsfunktionsanforderungen 46

6 Sicherheitsprozesspakete (SPP) 46
6.1 Allgemeines 46
6.2 Sichere Entwicklung 47
6.2.1 Anforderung 47
6.2.2 Wert 47
6.2.3 Überlegungen 47
6.3 Vertrauenswürdige Bereitstellung 47
6.3.1 Anforderung 47
6.3.2 Wert 47
6.3.3 Überlegungen 47

7 Sicherheits-Vertrauenswürdigkeitsanforderungen (SAR) 48
7.1 Sicherheits-Vertrauenswürdigkeitsanforderungen bei SESIP 48
7.2 Anforderungen der Sicherheitsvorgaben 48
7.2.1 Allgemeines 48
7.2.2 ASE_INT.SESIP 48

7.2.3 ASE_OBJ.SESIP 49
7.2.4 ASE_REQ.SESIP 49
7.2.5 ASE_TSS.SESIP 51
7.3 Anforderungen an die Leitfäden 52
7.3.1 AGD_PRE.SESIP 52
7.3.2 AGD_OPE.SESIP 52
7.4 Entwicklungsanforderungen 53
7.4.1 ADV_ARC.SESIP 53
7.4.2 ADV_TDS.SESIP 54
7.4.3 ADV_FSP.SESIP 54
7.4.4 ADV_IMP.SESIP 55
7.5 Anforderungen an die Lebenszyklusunterstützung 55
7.5.1 ALC_CMC.SESIP 55
7.5.2 ALC_CMS.SESIP 56
7.5.3 ALC_DEL.SESIP 56
7.5.4 ALC_DVS.SESIP 57
7.5.5 ALC_FLR.SESIP 57
7.5.6 ALC_TAT.SESIP 58
7.6 Prüfanforderungen 59
7.6.1 ATE_COV.SESIP 59
7.6.2 ATE_DPT.SESIP 59
7.6.3 ATE_FUN.SESIP 60
7.6.4 ATE_IND.SESIP 60
7.7 Anforderungen an die Schwachstellenbewertung 61
7.7.1 Allgemeines 61
7.7.2 AVA_VAN.SESIP1 61
7.7.3 AVA_VAN.SESIP2 62
7.7.4 AVA_VAN.SESIP3 62
7.7.5 AVA_VAN.SESIP4 63
7.7.6 AVA_VAN.SESIP5 63

8 SESIP Vertrauenswürdigkeitsstufen 64
8.1 Allgemeines 64
8.2 SESIP Vertrauenswürdigkeitsstufe 1 (SESIP1) 64
8.2.1 Allgemeines 64
8.2.2 Ziele 65
8.2.3 Vertrauenswürdigkeitskomponenten 65
8.3 SESIP Vertrauenswürdigkeitsstufe 2 (SESIP2) 66
8.3.1 Allgemeines 66
8.3.2 Ziele 66
8.3.3 Vertrauenswürdigkeitskomponenten 67
8.4 SESIP Vertrauenswürdigkeitsstufe 3 (SESIP3) 67
8.4.1 Allgemeines 67
8.4.2 Ziele 68
8.4.3 Vertrauenswürdigkeitskomponenten 68
8.5 SESIP Vertrauenswürdigkeitsstufe 4 (SESIP4) 69
8.5.1 Allgemeines 69
8.5.2 Ziele 69
8.5.3 Vertrauenswürdigkeitskomponenten 69
8.6 SESIP Vertrauenswürdigkeitsstufe 5 (SESIP5) 70
8.6.1 Allgemeines 70
8.6.2 Ziele 70
8.6.3 Vertrauenswürdigkeitskomponenten 71

Anhang A (informativ) Fallbeispiel für die SESIP Evaluierung 72

Anhang B (informativ) Leitlinien — Bewertung des Angriffspotenzials 73
B.1 Grundsätze 73
B.1.1 Allgemeines 73

B.1.2 Identifizierungs- und Ausnutzungsphasen 73
B.1.3 Physische (lokale) Angriffe und Fernangriffe 73
B.2 Bewertung des Angriffspotenzials 73

Anhang C (informativ) Beispiele für Anwendungsfälle 76
C.1 Generische Beispiele 76
C.1.1 IoT Cloud-Konnektivitätsplattform 76
C.1.2 Vertrauensgrundlage (RoT, en: Roots of Trust) bei einem Mikrocontroller 79
C.2 Beispiele für spezifische Anwendungsfälle 81
C.2.1 Allgemeines 81
C.2.2 Sichere Aktualisierung eines Produkts (OTA) 81
C.2.3 Ein Produkt zur Blutzuckermessung (DTSec) 82

Anhang D (informativ) Vorlage für Sicherheitsvorgaben 85
D.1 Allgemeines 85
D.2 Titelblatt der Sicherheitsvorgaben 85
D.3 Einleitung 85
D.3.1 Allgemeines 85
D.3.2 ST-Verweisung 85
D.3.3 Plattformverweisung 86
D.3.4 Enthaltene Leitfäden 86
D.3.5 (Optional) Sonstige Zertifizierung 86
D.3.6 Funktionsübersicht und Beschreibung der Plattform 87
D.4 Sicherheitszielsetzungen für die Betriebsumgebung 87
D.4.1 Plattformzielsetzungen für die Betriebsumgebung 87
D.4.2 (Optional) Übernommene Zielsetzungen für die Betriebsumgebung 88
D.5 Sicherheitsanforderungen und Implementierung 88
D.5.1 Sicherheits-Vertrauenswürdigkeitsanforderungen 88
D.5.2 Sicherheitsfunktionsanforderungen 89
D.5.3 (Optional) Sicherheitsprozesspaket 90
D.5.4 (Optional) Zusätzliche Anforderungen an funktionale Sicherheit/Prozesse 91
D.6 Abbildung und Angemessenheitsbegründungen 92
D.6.1 Allgemeines 92
D.6.2 Angemessenheit von SESIP1 92
D.6.3 Angemessenheit von SESIP2 93
D.6.4 Angemessenheit von SESIP3 95
D.6.5 Angemessenheit von SESIP4 97
D.6.6 Angemessenheit von SESIP5 99

Anhang E (normativ) Leitlinien für die Zusammensetzung 102
E.1 Einleitung 102
E.2 SESIP Zusammensetzungsprozess 102
E.3 Aktivitäten zur Evaluierung der SESIP Zusammensetzung 103
E.3.1 Allgemeines 103
E.3.2 Leitlinien für den Entwickler des zu integrierenden Plattformteils 104
E.3.3 Leitlinien für den Evaluator des zu integrierenden Plattformteils 104
E.3.4 Leitlinien für den Entwickler der Zusammensetzung 105
E.3.5 Leitlinien für den Evaluator der Zusammensetzung 107

Anhang F (informativ) SESIP im gesamten Prozess der Produktsicherung 110
F.1 Einleitung 110
F.2 Domäne der Risikoanalyse 111
F.3 Domäne der Angriffsverfahren 111
F.4 Sicherheitsbewertung 111
F.5 Mängelbeseitigung 112

Literaturhinweise 113