E DIN EN ISO/IEC 19896-2:2022-10 (D/E)

Erscheinungsdatum: 2022-09-23

IT-Sicherheitstechniken - Kompetenzan forderungen an Tester und Evaluatoren von Informationssicherheit - Teil 2: Anforderungen an Wissen, Fähigkeiten und Effektivität für ISO/IEC 19790-Tester (ISO/IEC 19896-2:2018); Deutsche und Englische Fassung prEN ISO/IEC 19896-2:2022

IT security techniques - Competence requirements for information security testers and evaluators - Part 2: Knowledge, skills and effectiveness requirements for ISO/I EC 19790 testers (ISO/IEC 19896-2:2018); German and English version prEN ISO/IEC 19896-2:2022

Inhalt

Seite

Europäisches Vorwort 4
Vorwort 5
Einleitung 6
1 Anwendungsbereich 7
2 Normative Verweisungen 7
3 Begriffe 7
4 Abkürzungen 7
5 Aufbau dieses Dokuments 8
6 Wissen 8
6.1 Allgemeines 8
6.2 Tertiäre Ausbildung 8
6.2.1 Allgemeines 8
6.2.2 Technische Fachrichtungen 8
6.2.3 Fachbezogene Themen 9
6.3 Wissen über die Normen 13
6.3.1 Allgemeines 13
6.3.2 ISO/IEC 19790-Konzepte 13
6.3.3 ISO/IEC 24759 13
6.3.4 Zusätzliche ISO/IEC-Normen 14
6.4 Wissen über das Validierungsprogramm 14
6.4.1 Validierungsprogramm 14
6.5 Wissen über die Anforderungen der ISO/IEC 17025 16
7 Fertigkeiten 16
7.1 Allgemeines 16
7.2 Prüfung von Algorithmen 16
7.3 Prüfung der physischen Sicherheit 17
7.4 Seitenkanalanalyse 17
7.5 Technologietypen 17
8 Erfahrung 17
8.1 Allgemeines 17
8.2 Nachweis der technischen Kompetenz für das Validierungsprogramm 17
8.2.1 Erfahrung mit der Durchführung von Prüfungen 17
8.2.2 Erfahrung mit bestimmten Technologietypen 17
9 Ausbildung 17
10 Effektivität 18
Anhang A (informativ) **Beispiel für ein ISO/IEC 24759-Testerprotokoll** 19
Anhang B (informativ) **Ontologie der Technologietypen und der zugehörigen Wissensbestände** . 20
B.1 Allgemeines 20
B.2 Technologietypen 20
B.2.1 Allgemeines 20
B.2.2 Software/Firmware 20
Anhang C (informativ) **Spezifisches Wissen im Zusammenhang mit der Sicherheit von kryptographischen Modulen** 24

C.1 Allgemeines . . . 24
C.2 Spezifikation des kryptographischen Moduls . . . 24
C.2.1 Allgemeines . . . 24
C.2.2 Puffer . . . 24
C.2.3 Sicherheitsrelevante Komponenten . . . 25
C.2.4 Identifizierung von programmierbaren Schnittstellen, Debugging-Schnittstellen und verdeckten Kanälen . . . 25
C.2.5 Identifizierung von genehmigten und nicht genehmigten Sicherheitsfunktionen . . . 25
C.2.6 Ausschluss von Komponenten . . . 25
C.2.7 Eingeschränkter Betrieb . . . 26
C.3 Schnittstellen des kryptographischen Moduls . . . 27
C.3.1 Überblick . . . 27
C.3.2 Abstand der Eingabedaten von den Ausgabedaten . . . 28
C.3.3 Wissen über kritische Sicherheitsfunktionen, Dienste oder sicherheitsrelevante Dienste 28
C.3.4 Vertrauenswürdiger Kanal . . . 28
C.4 Rollen, Dienste und Authentifizierung . . . 29
C.4.1 Allgemeines . . . 29
C.4.2 Dienste . . . 29
C.4.3 Authentifizierung . . . 30
C.5 Sicherheit der Software/Firmware . . . 31
C.6 Betriebsumgebung . . . 31
C.6.1 Prozessspeicherverwaltung . . . 31
C.6.2 Laden . . . 31
C.6.3 Verknüpfen . . . 31
C.6.4 Virtueller Speicher . . . 31
C.7 Physische Sicherheit . . . 31
C.8 Nicht-invasive Sicherheit . . . 31
C.9 Handhabung sensibler Sicherheitsparameter . . . 32
C.9.1 Allgemeines . . . 32
C.9.2 Kennwort gegenüber kryptographischem Schlüssel . . . 32
C.9.3 Entropie gegenüber dem Wissen der Angreifer . . . 32
C.9.4 SSP-Hierarchie . . . 33
C.9.5 Autorisierte Rollen für das SSP-Management . . . 33
C.9.6 Löschen . . . 34
C.10 Selbsttests . . . 34
C.10.1 Allgemeines . . . 34
C.10.2 Kritische Funktionen . . . 35
C.10.3 Vorbetriebliche Integritätsprüfung der Software/Firmware . . . 36
C.10.4 Bedingte Selbsttests des kryptographischen Algorithmus . . . 37
C.10.5 Paarweise Konsistenzprüfung . . . 37
C.11 Vertrauenswürdiger Lebenszyklus . . . 37
C.11.1 Allgemeines . . . 37
C.11.2 Konfigurationsmanagement . . . 37
C.11.3 Endlicher Automat . . . 38
C.11.4 Entwicklung . . . 38
C.11.5 Prüfung von Anbietern . . . 40
C.11.6 Auslieferung und Betrieb . . . 41
C.11.7 Ende der Nutzungsdauer . . . 42
C.11.8 Leitfäden . . . 42
C.12 Abwehr anderer Angriffe . . . 42
Anhang D (informativ) Kompetenzanforderungen an ISO/IEC 19790-Validierer . . . 43
Literaturhinweise . . . 44

Bilder

Bild C.1 — Überblick über die Spezifikation des kryptographischen Moduls . . . 24
Bild C.2 — Beispiel für Zustandsübergänge, die eine eingeschränkte Funktionalität unterstützen 27
Bild C.3 — Überblick über die Schnittstellen des kryptographischen Moduls . . . 28
Bild C.4 — Überblick über Rollen, Dienste und Authentifizierung . . . 29
Bild C.5 — Überblick über die Zugangssteuerungsrichtlinie . . . 30
Bild C.6 — Überblick über das SSP-Management . . . 32
Bild C.7 — Überblick über die Selbsttests . . . 35