

DIN EN 17640:2022-12 (D)

Zeitlich festgelegte Cybersicherheitsevaluationsmethodologie für IKT-Produkte; Deutsche Fassung EN 17640:2022

Inhalt	Seite
Europäisches Vorwort.....	5
Einleitung	6
1 Anwendungsbereich.....	8
2 Normative Verweisungen	8
3 Begriffe	8
4 Konformität.....	10
5 Allgemeine Konzepte	13
5.1 Anwendung dieser Methodologie	13
5.2 Wissen über den TOE	13
5.3 Evaluierung des Entwicklungsprozesses.....	13
5.4 Angriffspotential.....	14
5.5 Aufbau von Wissen.....	14
6 Evaluierungsaufgaben	15
6.1 Vollständigkeitsprüfung	15
6.1.1 Ziel.....	15
6.1.2 Evaluierungsmethode.....	15
6.1.3 Kompetenz des Evaluators.....	15
6.1.4 Workunits der Evaluatoren	15
6.2 Evaluierung des FIT-Schutzprofils.....	15
6.2.1 Ziel.....	15
6.2.2 Evaluierungsmethode.....	16
6.2.3 Kompetenz des Evaluators.....	16
6.2.4 Workunits der Evaluatoren	16
6.3 Überprüfung der Sicherheitsfunktionalitäten.....	17
6.3.1 Ziel.....	17
6.3.2 Evaluierungsmethode.....	17
6.3.3 Kompetenz des Evaluators.....	17
6.3.4 Workunits der Evaluatoren	17
6.4 Evaluierung der FIT-Sicherheitsvorgabe.....	17
6.4.1 Ziel.....	17
6.4.2 Evaluierungsmethode.....	18
6.4.3 Kompetenz des Evaluators.....	18
6.4.4 Workunits der Evaluatoren	18
6.5 Entwicklungsdokumentation	19
6.5.1 Ziel.....	19
6.5.2 Evaluierungsmethode.....	19
6.5.3 Kompetenz des Evaluators.....	19
6.5.4 Workunits	20
6.6 Evaluierung der TOE-Installation	20
6.6.1 Ziel.....	20
6.6.2 Evaluierungsmethode.....	20
6.6.3 Kompetenz des Evaluators.....	20
6.6.4 Workunits der Evaluatoren	20
6.7 Konformitätsprüfung.....	21

6.7.1	Ziel.....	21
6.7.2	Evaluierungsmethode.....	21
6.7.3	Kompetenz des Evaluators.....	21
6.7.4	Workunits der Evaluatoren.....	21
6.8	Schwachstellenprüfung.....	23
6.8.1	Ziel.....	23
6.8.2	Evaluierungsmethode.....	23
6.8.3	Kompetenz des Evaluators.....	23
6.8.4	Workunits der Evaluatoren.....	24
6.9	Erweiterte Schwachstellenprüfung.....	24
6.9.1	Ziel.....	24
6.9.2	Evaluierungsmethode.....	25
6.9.3	Kompetenz des Evaluators.....	25
6.9.4	Workunits der Evaluatoren.....	25
6.10	Penetrationsprüfung.....	27
6.10.1	Ziel.....	27
6.10.2	Evaluierungsmethode.....	27
6.10.3	Kompetenz des Evaluators.....	28
6.10.4	Workunits der Evaluatoren.....	28
6.11	Grundlegende Kryptoanalyse.....	29
6.11.1	Ziel.....	29
6.11.2	Evaluierungsmethode.....	29
6.11.3	Kompetenz des Evaluators.....	30
6.11.4	Workunits der Evaluatoren.....	30
6.12	Erweiterte Kryptoanalyse.....	31
6.12.1	Ziel.....	31
6.12.2	Evaluierungsmethode.....	31
6.12.3	Kompetenz des Evaluators.....	31
6.12.4	Workunits der Evaluatoren.....	31
Anhang A (informativ) Beispiel für die Struktur einer FIT-Sicherheitsvorgabe (FIT-ST).....		34
A.1	Allgemeines.....	34
A.2	Beispiel für die Struktur.....	34
A.3	Typische Inhalte einer FIT-ST.....	35
Anhang B (normativ) Das Konzept eines FIT-Schutzprofils (FIT-PP).....		36
B.1	Allgemeines.....	36
B.2	Ziel und Grundlagen eines FIT-PP.....	36
B.3	Anleitung für Schemata zur Implementierung des FIT-PP-Konzepts.....	36
Anhang C (informativ) Annahmekriterien.....		37
C.1	Einleitung.....	37
C.2	Identifizierung, Authentifizierungskontrolle und Zugriffskontrolle.....	37
C.3	Sicherer Systemstart (Secure Boot).....	40
C.4	Kryptographie.....	40
C.5	Sicherer Zustand nach Ausfall.....	41
C.6	Geringste Funktionalität.....	43
C.7	Aktualisierungsmechanismus.....	43
Anhang D (informativ) Anleitung für die Integration der Methodologie in ein Schema.....		45
D.1	Allgemeines.....	45
D.1.1	Einleitung.....	45
D.1.2	Durchführen einer Risikobeurteilung, Überprüfung der zu betrachtenden vertikalen Domäne.....	45
D.1.3	Zuordnen des Angriffspotentials zu den CSA-Vertrauenswürdigkeitsstufen.....	45
D.1.4	Auswählen der für diese CSA-Vertrauenswürdigkeitsstufe erforderlichen Evaluierungsaufgaben.....	45
D.1.5	Überprüfen und Festlegen der Parameter für die Arbeitsaufgaben.....	45
D.1.6	Mögliche Auswahl von zusätzlichen oder höherwertigen Arbeitsaufgaben.....	46
D.1.7	Überprüfen und Festlegen der Parameter für die zusätzlichen Arbeitsaufgaben.....	46

D.1.8	Erstellen und Pflegen weiterer Schemaanforderungen und -leitlinien.....	46
D.2	Beispiel	47
Anhang E (informativ) Parameter der Methodologie und der Evaluierungsaufgaben		50
E.1	Allgemeines.....	50
E.2	Parameter der Methodologie	50
E.3	Parameter der Evaluierungsaufgaben.....	50
E.3.1	Parameter für 6.1 „Vollständigkeitsprüfung“	50
E.3.2	Parameter für 6.2 „Evaluierung des FIT-Schutzprofils“	50
E.3.3	Parameter für 6.3 „Überprüfung der Sicherheitsfunktionalitäten“	50
E.3.4	Parameter für 6.4 „Evaluierung der Sicherheitsvorgabe“	50
E.3.5	Parameter für 6.5 „Entwicklungsdokumentation“	50
E.3.6	Parameter für 6.6 „Evaluierung der TOE-Installation“	51
E.3.7	Parameter für 6.7 „Konformitätsprüfung“	51
E.3.8	Parameter für 6.8 „Schwachstellenprüfung“	51
E.3.9	Parameter für 6.9 „Erweiterte Schwachstellenprüfung“	51
E.3.10	Parameter für 6.10 „Penetrationsprüfung“	51
E.3.11	Parameter für 6.11 „Grundlegende Kryptoanalyse“	51
E.3.12	Parameter für 6.12 „Erweiterte Kryptoanalyse“	51
Anhang F (normativ) Berechnung des Angriffspotentials		52
F.1	Allgemeines.....	52
F.2	Faktoren für das Angriffspotential	52
F.3	Numerische Faktoren für das Angriffspotential.....	52
F.3.1	Allgemeines.....	52
F.3.2	Standardbewertungstabelle	53
F.3.3	Anpassung der Bewertungstabelle.....	54
Anhang G (normativ) Berichterstattung über die Ergebnisse einer Evaluierung.....		56
G.1	Allgemeines.....	56
G.2	Schriftliche Berichterstattung.....	56
G.3	Mündliche Verteidigung der erzielten Ergebnisse	56
Literaturhinweise		58