

E DIN EN 17640:2021-07 (D/E)

Erscheinungsdatum: 2021-06-18

Cybersicherheitsevaluationsmethodologie für IKT-Produkte; Deutsche und Englische Fassung prEN 17640:2021

Fixed time cybersecurity evaluation methodology for ICT products; German and English version prEN 17640:2021

Inhalt	Seite
Europäisches Vorwort.....	5
Einleitung	6
1 Anwendungsbereich.....	8
2 Normative Verweisungen	8
3 Begriffe	8
4 Konformität.....	10
5 Allgemeine Begriffe	12
5.1 Anwendung dieser Methodologie	12
5.2 Wissen über den TOE	12
5.3 Evaluierung des Entwicklungsprozesses.....	13
5.4 Angriffspotential.....	13
5.5 Aufbau von Wissen.....	14
6 Evaluierungsarbeitsaufgaben	14
6.1 Vollständigkeitsprüfung	14
6.1.1 Ziel.....	14
6.1.2 Evaluierungsverfahren.....	14
6.1.3 Qualifikation des Evaluators	14
6.1.4 Workunits der Evaluatoren	14
6.2 Evaluierung des Schutzprofils.....	15
6.2.1 Ziel.....	15
6.2.2 Evaluierungsverfahren.....	15
6.2.3 Qualifikation des Evaluators	15
6.2.4 Workunits der Evaluatoren	15
6.3 Evaluierung der Sicherheitsvorgabe.....	16
6.3.1 Ziel.....	16
6.3.2 Evaluierungsverfahren.....	16
6.3.3 Qualifikation des Evaluators	16
6.3.4 Workunits der Evaluatoren	16
6.4 Überprüfung der Sicherheitsfunktionalitäten.....	18
6.4.1 Ziel.....	18
6.4.2 Evaluierungsverfahren.....	18
6.4.3 Qualifikation des Evaluators	18
6.4.4 Workunits der Evaluatoren - Workunit 1.....	18
6.5 Entwicklungsdokumentation	18
6.5.1 Ziel.....	18
6.5.2 Evaluierungsverfahren.....	18
6.5.3 Qualifikation des Evaluators	19
6.5.4 Workunits	19
6.6 Evaluierung der TOE-Installation	19
6.6.1 Ziel.....	19
6.6.2 Evaluierungsverfahren.....	19

6.6.3	Qualifikation des Evaluators	19
6.6.4	Workunits der Evaluatoren	19
6.7	Konformitätsprüfung	20
6.7.1	Ziel	20
6.7.2	Evaluierungsverfahren	20
6.7.3	Qualifikation des Evaluators	20
6.7.4	Workunits der Evaluatoren	21
6.8	Anfälligkeitsüberprüfung	22
6.8.1	Ziel	22
6.8.2	Evaluierungsverfahren	22
6.8.3	Qualifikation des Evaluators	22
6.8.4	Workunits der Evaluatoren	23
6.9	Anfälligkeitsprüfung	23
6.9.1	Ziel	23
6.9.2	Evaluierungsverfahren	24
6.9.3	Qualifikation des Evaluators	24
6.9.4	Workunits der Evaluatoren	24
6.10	Penetrationstest	26
6.10.1	Ziel	26
6.10.2	Evaluierungsverfahren	26
6.10.3	Qualifikation des Evaluators	27
6.10.4	Workunits der Evaluatoren	28
6.11	Grundlegende Kryptoanalyse	28
6.11.1	Ziel	28
6.11.2	Evaluierungsverfahren	29
6.11.3	Qualifikation des Evaluators	29
6.11.4	Workunits der Evaluatoren	29
6.12	Erweiterte Kryptoanalyse	30
6.12.1	Ziel	30
6.12.2	Evaluierungsverfahren	30
6.12.3	Qualifikation des Evaluators	30
6.12.4	Workunits der Evaluatoren	31
Anhang A (informativ) Beispiel für die Struktur einer Sicherheitsvorgabe		33
A.1	Allgemeines	33
A.2	Beispiel für die Struktur	33
A.3	Typische Inhalte einer ST	34
Anhang B (normativ) Der Begriff eines Schutzprofils		35
B.1	Allgemeines	35
B.2	Ziel und Grundlagen eines Schutzprofils (PP)	35
B.3	Leitlinien für Schemata zur Implementierung des PP-Begriffs	35
Anhang C (informativ) Annahmekriterien		36
C.1	Einleitung	36
C.2	Identifizierung, Authentifizierungskontrolle und Zugriffskontrolle	36
C.3	Sicherer Systemstart (Secure Boot)	39
C.4	Kryptographie	40
C.5	Sicherer Zustand nach Ausfall	41
C.6	Geringste Funktionalität	42
C.7	Aktualisierungsmechanismus	43
Anhang D (informativ) Leitlinien für die Integration der Methodologie in ein Schema		44
D.1	Allgemeines	44
D.1.1	Einleitung	44
D.1.2	Durchführen einer Risikobeurteilung, Überprüfung der zu betrachtenden vertikalen Domäne	44
D.1.3	Zuordnen des Angriffspotentials zu den CSA-Stufen	44
D.1.4	Auswählen der für diese Stufe erforderlichen Evaluierungsarbeitsaufgaben	44
D.1.5	Überprüfen und Festlegen der Parameter für die Arbeitsaufgaben	44

D.1.6	Mögliche Auswahl von zusätzlichen oder übergeordneten Arbeitsaufgaben	45
D.1.7	Überprüfen und Festlegen der Parameter für die zusätzlichen Arbeitsaufgaben	45
D.1.8	Erstellen und Pflegen weiterer Schemaanforderungen und -leitlinien.....	45
D.2	Beispiel	46
Anhang E (informativ) Parameter der Methodologie und der Evaluierungsarbeitsaufgaben		49
E.1	Allgemeines	49
E.2	Parameter der Methodologie	49
E.3	Parameter der Evaluierungsarbeitsaufgaben.....	49
E.3.1	Parameter für 6.1 „Vollständigkeitsprüfung“	49
E.3.2	Parameter für 6.2 „Evaluierung des Schutzprofils“	49
E.3.3	Parameter für 6.3 „Evaluierung der Sicherheitsvorgabe“	49
E.3.4	Parameter für 6.4 „Überprüfung der Sicherheitsfunktionalitäten“.....	49
E.3.5	Parameter für 6.5 „Entwicklungsdokumentation“	49
E.3.6	Parameter für 6.6 „Evaluierung der TOE-Installation“	50
E.3.7	Parameter für 6.7 „Konformitätsprüfung“	50
E.3.8	Parameter für 6.8 „Anfälligkeitsüberprüfung“	50
E.3.9	Parameter für 6.9 „Anfälligkeitsprüfung“	50
E.3.10	Parameter für 6.10 „Penetrationstest“.....	50
E.3.11	Parameter für 6.11 „Grundlegende Kryptoanalyse“	50
E.3.12	Parameter für 6.12 „Erweiterte Kryptoanalyse“	50
Anhang F (normativ) Berechnung des Angriffspotentials		51
F.1	Allgemeines	51
F.2	Faktoren für das Angriffspotential	51
F.3	Numerische Faktoren für das Angriffspotential.....	51
F.3.1	Standardbewertungstabelle	52
F.3.2	Anpassung der Bewertungstabelle.....	53
Anhang G (normativ) Berichterstattung über die Ergebnisse einer Evaluierung.....		55
G.1	Allgemeines	55
G.2	Schriftliche Berichterstattung.....	55
G.3	Mündliche Verteidigung der erzielten Ergebnisse	55
Literaturhinweise		57