E DIN EN 40000-1-2:2026-03 (D/E)

Erscheinungsdatum: 2026-02-20

Cybersicherheitsanforderungen für Produkte mit digitalen Elementen - Teil 1-2: Grundsätze für die Cyberresilienz; Deutsche und Englische Fassung prEN 40000-1-2:2025

Cybersecurity requirements for products with digital elements - Part 1-2: Principles for cyber resilience; German and English version prEN 40000-1-2:2025

Inhalt

Seite

Europäisches Vorwort 8

1 Anwendungsbereich 9

2 Normative Verweisungen 9

3 Begriffe 9

4 Einleitung 9

5 Grundsätze der Cybersicherheit 10
5.1 Allgemeines 10
5.2 Risikobasiertes Cybersicherheitskonzept 11
5.2.1 Kurzbeschreibung 11
5.2.2 Leitlinien 11
5.3 Sicherheit durch Gestaltung 12
5.3.1 Kurzbeschreibung 12
5.3.2 Leitlinien 12
5.4 Sicherheit durch Voreinstellung 13
5.4.1 Kurzbeschreibung 13
5.4.2 Leitlinien 13
5.5 Transparenz 13
5.5.1 Kurzbeschreibung 13
5.5.2 Leitlinien 13

6 Elemente des Risikomanagements 14
6.1 Allgemeines 14
6.2 Produktkontext 16
6.2.1 Allgemeines 16
6.2.2 Ausgangsinformationen 18
6.2.3 Anforderungen 18
6.2.4 Ergebnis 19
6.2.5 Beurteilungskriterien 19
6.3 Risikoakzeptanzkriterien und Risikomanagementmethodik 19
6.3.1 Allgemeines 19
6.3.2 Ausgangsinformationen 21
6.3.3 Anforderungen 21
6.3.4 Ergebnis 21
6.3.5 Beurteilungskriterien 22
6.4 Risikobeurteilung 22
6.4.1 Allgemeines 22
6.4.2 Identifizierung von Vermögenswerten und Cybersicherheitszielen 23
6.4.3 Identifizierung der Bedrohungen 24
6.4.4 Risikoabschätzung 25
6.4.5 Risikobewertung 26
6.5 Risikobehandlung 27
6.5.1 Allgemeines 27
6.5.2 Ausgangsinformationen 28

6.5.3 Anforderungen ... 28
6.5.4 Ergebnis ... 29
6.5.5 Beurteilungskriterien ... 29
6.6 Risikokommunikation ... 29
6.6.1 Allgemeines ... 29
6.6.2 Ausgangsinformationen ... 30
6.6.3 Anforderungen ... 30
6.6.4 Ergebnis ... 30
6.6.5 Beurteilungskriterien ... 30
6.7 Risikoüberwachung und -überprüfung ... 31
6.7.1 Allgemeines ... 31
6.7.2 Ausgangsinformationen ... 31
6.7.3 Anforderungen ... 31
6.7.4 Ergebnis ... 32
6.7.5 Beurteilungskriterien ... 32

7 Cybersicherheitstätigkeiten ... 32
7.1 Allgemeines ... 32
7.2 Planung der Produktcybersicherheit ... 33
7.2.1 Allgemeines ... 33
7.2.2 Ausgangsinformationen ... 33
7.2.3 Anforderungen ... 33
7.2.4 Ergebnis ... 33
7.2.5 Beurteilungskriterien ... 33
7.3 Cybersicherheitsanforderungen an Produkte ... 34
7.3.1 Allgemeines ... 34
7.3.2 Ausgangsinformationen ... 35
7.3.3 Anforderungen ... 35
7.3.4 Ergebnis ... 35
7.3.5 Beurteilungskriterien ... 35
7.4 Architektur und Gestaltung der Cybersicherheit ... 36
7.4.1 Allgemeines ... 36
7.4.2 Ausgangsinformationen ... 36
7.4.3 Anforderungen ... 36
7.4.4 Ergebnis ... 36
7.4.5 Beurteilungskriterien ... 36
7.5 Sichere Implementierung ... 37
7.5.1 Allgemeines ... 37
7.5.2 Ausgangsinformationen ... 38
7.5.3 Anforderungen ... 38
7.5.4 Ergebnis ... 38
7.5.5 Beurteilungskriterien ... 39
7.6 Verifizierung und Validierung der Cybersicherheit ... 39
7.6.1 Allgemeines ... 39
7.6.2 Ausgangsinformationen ... 40
7.6.3 Anforderungen ... 41
7.6.4 Ergebnis ... 41
7.6.5 Beurteilungskriterien ... 41
7.7 Sichere Produktion und Verteilung ... 42
7.7.1 Allgemeines ... 42
7.7.2 Digitale Produktion ... 42
7.7.3 Herstellung ... 44
7.8 Management von Cybersicherheitsproblemen ... 45
7.8.1 Allgemeines ... 45
7.8.2 Ausgangsinformationen ... 46
7.8.3 Anforderungen ... 46
7.8.4 Ergebnis ... 46
7.8.5 Beurteilungskriterien ... 46
7.9 Produktüberwachung ... 46

7.9.1 Allgemeines ... 46
7.9.2 Ausgangsinformationen ... 47
7.9.3 Anforderungen ... 47
7.9.4 Ergebnis ... 47
7.9.5 Beurteilungskriterien ... 47
7.10 Planung der sicheren Außerbetriebnahme ... 48
7.10.1 Allgemeines ... 48
7.10.2 Ausgangsinformationen ... 48
7.10.3 Anforderungen ... 48
7.10.4 Ergebnis ... 49
7.10.5 Beurteilungskriterien ... 49
7.11 Cybersicherheitsmanagement für Komponenten von Drittanbietern ... 49
7.11.1 Allgemeines ... 49
7.11.2 Ausgangsinformationen ... 50
7.11.3 Anforderungen ... 50
7.11.4 Ergebnis ... 51
7.11.5 Beurteilungskriterien ... 51

Anhang A (informativ) Kohärenz mit vertikalen Normen ... 52
A.1 Elemente der Kohärenz ... 52

Anhang B (informativ) Beispiel für einen Cybersicherheitsanbietervertrag (CSSA) ... 53
B.1 Allgemeines ... 53
B.2 Beispiel-CSSA ... 54

Anhang C (informativ) Zusammenhang zwischen dieser Europäischen Norm und den grundlegenden Cybersicherheitsanforderungen der Verordnung (EU) 2024/2847 ... 59
C.1 Allgemeines ... 59
C.2 Verweisung auf grundlegende Anforderungen ... 59
C.3 Zuordnung zu grundlegenden Anforderungen ... 59
C.4 Normative und informative Teile ... 64
C.5 Beurteilungskriterien ... 64

Anhang D (informativ) Barrierefreie und inklusive Cybersicherheit ... 65
D.1 Anwendungsbereich ... 65
D.2 Rechtlicher Hintergrund ... 65
D.3 Der Nutzer ... 65
D.4 Art der erforderlichen Interaktion ... 66
D.5 Folgen des Interaktionsverfahrens für die Cybersicherheit des Nutzers ... 66
D.6 Empfohlene Lösung für die Sicherstellung einer maximalen Cybersicherheit für die potentiellen Nutzer ... 67
D.7 Kommunikation mit dem Nutzer ... 67

Literaturhinweise ... 68

Bilder

Bild 1 — Überblick über die Elemente des Risikomanagements ... 15

Bild B.1 — Beispiel für CSSA in der Lieferkette ... 53

Tabellen

Tabelle B.1 — Beispiel für einen CSSA ... 54

Tabelle C.1 — Zusammenhang zwischen dieser Europäischen Norm und Anhang I der Verordnung (EU) 2024/2847 [Amtsblatt der Europäischen Union L 60] ... 60

Tabelle C.2 — Normativer Status der Struktur der einzelnen Abschnitte ... 64