E DIN EN 18037-2:2026-09 (D/E)

Erscheinungsdatum: 2026-08-21

Leitlinien für eine sektorale Bewertung der Cybersicherheit - Teil 2: Anwendung der Ergebnisse der sektoralen Bewertung der Cybersicherheit durch Hersteller von IKT-Produkten; Deutsche und Englische Fassung prEN 18037-2:2026

Guidelines on a sectoral cybersecurity assessment - Part 2: Application of sectoral cybersecurity assessment results by ICT product manufacturers; German and English version prEN 18037-2:2026

Inhalt

Seite

Europäisches Vorwort ... 8

Einleitung ... 9

1 Anwendungsbereich ... 10

2 Normative Verweisungen ... 10

3 Begriffe ... 10

4 Symbole und Abkürzungen ... 11

5 Überblick über Bewertungen nach EN 18037 aus Sicht der Hersteller von IKT-Produkten ... 11
5.1 IKT-Produkte als Teil des sektoralen IKT-Systems ... 11
5.2 Rolle des Produktherstellers bei der sektoralen Cybersicherheit und Risikobewertung ... 11
5.3 Möglichkeiten von EN 18037 zur Unterstützung von Herstellern von IKT-Produkten ... 12
5.4 Unterstützung für marktübergreifende IKT-Produkte ... 13
5.5 Auswirkung der Entscheidungen der Interessengruppen zur Risikobehandlung auf IKT-Produkte ... 14

6 Für Hersteller von IKT-Produkten erforderliche sektorale Informationen ... 14

7 Anleitung zur Anwendung von EN 18037 durch sektorale Interessengruppen ... 15
7.1 Allgemeines ... 15
7.2 Leitlinien zu allgemeinen Aspekten der sektoralen Bewertung ... 16
7.2.1 Einschätzungen und Annahmen ... 16
7.2.2 Unparteilichkeit und diskriminierungsfreier Zugang ... 16
7.3 Anleitung zur Festlegung des Sektorkontexts ... 17
7.3.1 Einführung in den Marktsektor ... 17
7.3.2 Typen von sektoralen Interessengruppen sowie deren Rollen und Verantwortlichkeiten ... 18
7.3.3 Geschäfts- und Betriebsprozesse, Identifizierung der Ziele der Interessengruppen ... 19
7.3.4 Architektur des sektoralen Systems ... 20
7.3.5 Teilsysteme und Identifizierung von Informationswerten, funktionalen und unterstützenden Werten ... 21
7.3.6 Dokumentation der sektoralen Bedrohungsinformationen (CTI) ... 22
7.4 Anleitung zur Durchführung der Bewertung der Primärwerte ... 23
7.4.1 Allgemeine Anleitung ... 23
7.4.2 Ermittlung von Risiken, Festlegung von Bewertungsszenarien für jeden Geschäftsprozess ... 24
7.4.3 Bewertung und Einstufung von Risiken für Primärwerte ... 24
7.4.4 Identifizierung der Anforderungen an die Sicherheits- und Vertrauenswürdigkeitsstufe für jedes Risikoszenario ... 25
7.4.5 Entscheidungen zur Risikobehandlung je Risikoszenario ... 25
7.5 Anleitung für die Bewertung der unterstützenden Werte von IKT-Produkten ... 27
7.5.1 Allgemeine Anleitung ... 27
7.5.2 Definition und Dokumentation von Risikominderungsmaßnahmen auf Systemebene ... 27
7.5.3 Identifizierung von IKT-Produkten für die Bewertung der unterstützenden Werte ... 27
7.5.4 Aggregation von Informationen zu IKT-Produkten ... 28
7.5.5 Neubewertung der unterstützenden Werte je Risikoszenario ... 28

7.5.6 Aggregation der Ergebnisse der Neubewertung je IKT-Produkt ... 29
7.6 Zuordnung der erkannten Sicherheits- und Vertrauenswürdigkeitsanforderungen ... 29
7.6.1 Allgemeines ... 29
7.6.2 Anleitung zur Durchführung der Lückenanalyse von unterstützenden Werten ... 29
7.6.3 Identifizierung potentieller Lösungen ... 31
7.6.4 Anleitung für den Fall, dass keine Lösungen für produktspezifische Lücken vorliegen ... 31
7.7 Pflege des Bewertungsberichts ... 31

8 Anleitung zur Anwendung von EN 18037 durch Produkthersteller ... 32
8.1 Allgemeines ... 32
8.2 Anleitung für Produkthersteller zur Dokumentation des Sektorkontexts ... 32
8.2.1 Allgemeine Anleitung ... 32
8.2.2 Einschätzung der relevanten Ziele und Werte auf der Grundlage der bestimmungsgemäßen Nutzung des Produkts ... 32
8.2.3 Einschätzung der sektoralen Bedrohungsinformationen (CTI) ... 33
8.3 Anleitung für Produkthersteller zur Durchführung der Bewertung von Primärwerten ... 33
8.4 Anleitung für Produkthersteller zur Durchführung der Bewertung von unterstützenden Werten ... 34
8.5 Zuordnung der ermittelten Sicherheits- und Vertrauenswürdigkeitsanforderungen ... 34

Anhang A (informativ) Beispiel für die Bewertung eines fiktiven sektoralen Systems ... 35
A.1 Allgemeines ... 35
A.2 Kontextdokumentation des fiktiven sektoralen Systems ... 35
A.2.1 Einführung in den fiktiven Marktsektor ... 35
A.2.2 Typen von sektoralen Interessengruppen sowie deren Rollen und Verantwortlichkeiten ... 36
A.2.3 Geschäfts- und Betriebsprozesse, Identifizierung der Ziele der Interessengruppen ... 37
A.2.4 Architektur des fiktiven sektoralen Systems ... 40
A.2.5 Identifizierung von Teilsystemen ... 42
A.2.6 Dokumentation sektoraler Bedrohungsinformationen (CTI) ... 45
A.3 Bewertung der Primärwerte des fiktiven sektoralen Systems ... 48
A.3.1 Risikobewertung BP1 „Vertriebsprozess für Dienstleistungskunden“ ... 48
A.4 Dokumentation von Entscheidungen zur Risikobehandlung ... 56
A.4.1 Allgemeines ... 56
A.4.2 B1: Entscheidungen zur Risikobehandlung für Risiko R-BP1.1 „Kompromittierung von Berechtigungen“ ... 56
A.5 Bewertung der unterstützenden Werte des fiktiven sektoralen Systems ... 57
A.5.1 Dokumentation von Minderungsmaßnahmen auf Systemebene ... 57
A.5.2 Identifizierung von IKT-Produkten für die Bewertung unterstützender Werte ... 59
A.5.3 Bewertung des unterstützenden Werts „Berechtigungsmanagementsystem“ ... 60

Literaturhinweise ... 66

Bilder

Bild A.1 — Typen von sektoralen Interessengruppen ... 37

Bild A.2 — Ausgewählte Geschäftsprozesse ... 38

Bild A.3 — Funktionale Systemarchitektur ... 40

Bild A.4 — Ausgewählte Teilsysteme „Online-Vertrieb an Kunden“ und „Zugang zum Kundendienst“ ... 43

Bild A.5 — Datenfluss BP1 „Online-Vertrieb an Kunden“ ... 43

Tabellen

Tabelle A.1 — Beschreibung von BP1 als Beispiel für die Dokumentation von Geschäftsprozessen 38

Tabelle A.2 — BP1, Ziele der Interessengruppen 39

Tabelle A.3 — Zuordnung zwischen IKT-Funktionen und IKT-Produkten 41

Tabelle A.4 — Teilsystem BP1, Informationen und Unterstützungsfunktionen 44

Tabelle A.5 — Teilsystem BP1, unterstützende Werte und deren bestimmungsgemäße Nutzung 44

Tabelle A.6 — Einschätzung des Motivationniveaus des Angreifertyps 46

Tabelle A.7 — BP1: Verknüpfen von Werten mit den Zielen der Interessengruppen 49

Tabelle A.8 — BP1: Identifizierung von Risiken 49

Tabelle A.9 — BP1: Angreiferszenario AS-BP1.1 „Cyberkriminelle“ 50

Tabelle A.10 — BP1: Angreiferszenario AS-BP1.2 „Betrügerische Dienstleistungskunden“ 51

Tabelle A.11 — BP1: Risikoszenario RS-BP1.1.1 „Kompromittierung zahlreicher Berechtigungen“ 52

Tabelle A.12 — BP1: Risikoszenario RS-BP1.1.2 „Kompromittierung einzelner Berechtigungen“ 52

Tabelle A.13 — BP1: Wirkungsklasse für das Risiko RS-BP1.1 „Kompromittierung von Berechtigungen“ 53

Tabelle A.14 — BP1: MRC für das Risiko R-BP1.1 „Kompromittierung von Berechtigungen“ 54

Tabelle A.15 — BP1: Vorläufige CSL und CAR für das Risiko RS-BP1.1 „Kompromittierung von Berechtigungen“ 55

Tabelle A.16 — BP1: RTD-B1.1 56

Tabelle A.17 — IKT-Produkte zur Bewertung unterstützender Werte 59

Tabelle A.18 — Bestimmungsgemäße Nutzung des IKT-Produkts „Berechtigungsmanagementsystem“ 60

Tabelle A.19 — Aggregation von szenariospezifischen Informationen für das IKT-Produkt „Berechtigungsmanagementsystem“ 61

Tabelle A.20 — Anforderungen an das Produkt „Berechtigungsmanagementsystem“ in RS-BP1.1.1 64