E DIN EN 18037:2023-12 (D/E)

Erscheinungsdatum: 2023-11-17

Leitlinien für ein sektorales Cybersecurity Assessment; Deutsche und Englische Fassung prEN 18037:2023

Guidelines on a sectoral cybersecurity assessment; German and English version prEN 18037:2023

Inhalt

Seite

Europäisches Vorwort ... 9

Einleitung ... 10

1 Anwendungsbereich ... 13

2 Normative Verweisungen ... 13

3 Begriffe ... 13
3.1 Allgemeine Begriffe ... 13
3.2 Begriffe im Zusammenhang mit Organisation ... 14
3.3 Begriffe im Zusammenhang mit einem sektoralen Cybersicherheitsansatz ... 15
3.4 Begriffe im Zusammenhang mit Risiko ... 16

4 Abkürzungen ... 18

5 Sektorales Cybersecurity Assessment ... 18
5.1 Anwendung der Methodik für sektorale Cybersecurity Assessments ... 18
5.2 Grundsätze und neue Potentiale ... 20

6 Sektorale Darstellung von Risiken ... 23
6.1 Sektorale IKT-Systeme ... 23
6.1.1 Sektorale IKT-Systemkomponenten und ihre Beziehungen ... 23
6.1.2 Mehrschichtige Architektur sektoraler IKT-Systeme ... 24
6.1.3 Risikobasierte Definitionen von Cybersecurity- und Vertrauenswürdigkeitsanforderungen in sektoralen Systemen ... 26
6.1.4 Relevanz der sektoralen IKT-Systemarchitektur für die Risikobewertung ... 26
6.1.5 Cybersecurity-Zertifizierung sektoraler IKT-Systeme ... 27
6.2 Einheitliche sektorale Risikobewertung ... 28
6.3 Durchführung einer sektoralen Risikobewertung ... 29
6.3.1 Allgemeines ... 29
6.3.2 Wahl des Ansatzes ... 31
6.3.3 Identifizierung von Geschäftsprozessen, -zielen und -anforderungen ... 31
6.3.4 Identifizierung von Primärwerten und unterstützenden Werten ... 31
6.3.5 Definition von Risikoszenarien ... 31
6.3.6 Bewertung der Folgen in Risikoszenarien ... 32
6.3.7 Bewertung der Wahrscheinlichkeit in Risikoszenarien ... 33
6.3.8 Integration der Angreiferperspektive: Bewertung des Angriffspotentials ... 34
6.3.9 Erneute Risikobewertung für unterstützende Werte ... 35

7 Normalisierte Darstellung von Risiko, Cybersecurity und Vertrauenswürdigkeit ... 35
7.1 Ergebnisse von Risikobewertungen: Meta-Risikoklassen ... 35
7.2 Risikobasierte Definition von allgemeinen Sicherheitsstufen und Auswahl von Sicherheitsmaßnahmen ... 36
7.2.1 Allgemeines ... 36
7.2.2 Einführung von allgemeinen Sicherheitsstufen (CSL) ... 36
7.2.3 Einsatz von Meta-Risikoklassen und allgemeinen Sicherheitsstufen zur sektoralen Risikobehandlung ... 37

7.2.4 Angriffspotential als Kriterium für die Auswahl der CSL von Maßnahmen ... 37
7.3 Einheitliche Implementierung von Vertrauenswürdigkeit ... 38
7.3.1 Einführung ... 38
7.3.2 Definition eines allgemeinen Vertrauenswürdigkeitsreferenzkonzepts basierend auf ISO/IEC 15408 ... 38
7.3.3 Anwendung des CTI-Konzepts zum Angriffspotential auf CAR ... 39

8 Zuordnung von Cybersecurity- und Vertrauenswürdigkeitsanforderungen zur Programmdarstellung ... 40

Anhang A (informativ) Beispiele für normalisierte Skalen bei der sektoralen Risikobewertung ... 41
A.1 Qualitativer Ansatz zur Bewertung der Folgen ... 41
A.2 Qualitativer Ansatz zur Wahrscheinlichkeitsbewertung ... 42
A.3 Qualitativer Ansatz zur Risikoeinschätzung ... 43
A.4 Qualitativer Ansatz zur Risikominderung ... 43
A.5 Meta-Risikoklassen durch eine Klassifizierung der allgemeinen Vertrauenswürdigkeitsreferenz adressieren ... 44

Anhang B (informativ) CTI-Grundlagen ... 45
B.1 Allgemeines ... 45
B.2 Angreifertypen ... 46
B.3 Merkmale der Angreifer ... 48
B.4 Kriterien für eine qualitative Einschätzung des Angriffspotentials ... 51
B.4.1 Merkmale: Gelegenheit ... 51
B.4.2 Merkmale: Mittel ... 55
B.4.3 Merkmal: Motive ... 59
B.5 Einschätzung des Angriffspotentials mithilfe des CTI-Ansatzes ... 62
B.5.1 Allgemeines ... 62
B.5.2 Merkmale: Gelegenheit ... 62
B.5.3 Merkmale: Mittel ... 63
B.5.4 Merkmale: Motive ... 64
B.5.5 Berechnung des Angriffspotentials (APL) ... 64
B.5.6 Eine Gleichwertigkeit zwischen CTI und ISO/IEC 18045 für die Einschätzung des Angriffspotentials finden ... 65

Anhang C (informativ) Anwendung des Ansatzes der allgemeinen Sicherheitsstufen — Beispiele ... 68
C.1 Allgemeines ... 68
C.2 Anwendungsbeispiel: Mobilgerät-basiertes Authentifizierungssystem ... 68
C.3 Anwendungsbeispiel: Schutz gegen geklonte Geräte und betrügerische Anbieter ... 70

Anhang D (informativ) Beispiel für die Zuordnung einer Vertrauenswürdigkeitsstufe ... 72

Literaturhinweise ... 73

Bilder

Bild 1 — Sektorales Cybersecurity Assessment ... 20

Bild 2 — Überblick über die vom sektoralen Cybersecurity Assessment genutzten und generierten Informationen ... 21

Bild 3 — Beziehung zwischen IKT-Dienstleistungen, IKT-Produkten und IKT-Prozessen ... 24

Bild 4 — Schichten eines sektoralen IKT-Systems ... 25

Bild 5 — Beziehung zwischen Geschäftsprozessen, Primärwerten und unterstützenden Werten ... 27

Bild 6 — Sektorale Risikobewertung ... 30

Bild B.1 — Merkmale des Angreifers **46**

Bild B.2 — Komponente zur Einschätzung des Angriffspotentials **48**

Tabellen

Tabelle 1 — Zuordnung der allgemeinen Vertrauenswürdigkeitsreferenz (CAR) **39**

Tabelle A.1 — Wirkungsklassen — Beispiel 1 ..... **41**

Tabelle A.2 — Wirkungsklassen je Risikobereich — Beispiel 2 ..... **41**

Tabelle A.3 — Wahrscheinlichkeitsbewertung — ein Beispiel **43**

Tabelle A.4 — Meta-Risikoklassen — Beispiel **43**

Tabelle A.5 — Allgemeine Sicherheitsstufen — Beziehungen zu Meta-Risikoklassen und Angriffspotentialen **44**

Tabelle A.6 — Kombinationen von MRC, AP und CAR — Beispiel **44**

Tabelle B.1 — Beschreibung des Angriffspotentials anhand von Systemzugriff und -wissen **48**

Tabelle B.2 — Beschreibung des Angriffspotentials anhand von Schwachstellen **49**

Tabelle B.3 — Beschreibung des Angriffspotentials in Abwesenheit bekannter Schwachstellen **49**

Tabelle B.4 — Beschreibung des Angriffspotentials anhand von Fähigkeiten und Ressourcen **49**

Tabelle B.5 — Beschreibung des Angriffspotentials anhand von Fähigkeitsmerkmalen **50**

Tabelle B.6 — Beschreibung des Angriffspotentials anhand der Wertwahrnehmung **50**

Tabelle B.7 — Beschreibung des Angriffspotentials anhand von Zielen **50**

Tabelle B.8 — Qualitativer Angriffswert nach Zugang/Zeit mit dem unterstützenden Wert zur Angriffsvorbereitung **51**

Tabelle B.9 — Qualitativer Angriffswert nach Zugang/Zeit mit dem unterstützenden Wert zur Angriffsdurchführung **52**

Tabelle B.10 — Qualitativer Angriffswert nach Wissen über den unterstützenden Wert **52**

Tabelle B.11 — Qualitativer Angriffswert nach Wissen über die Schwachstellen **53**

Tabelle B.12 — Qualitativer Angriffswert nach Zugang zur Quelle des unterstützenden Werts **54**

Tabelle B.13 — Qualitativer Angriffswert nach Fähigkeit, auf unterstützende Werte in der Lieferkette zuzugreifen/diese zu modifizieren **54**

Tabelle B.14 — Qualitativer Angriffswert nach Fähigkeit zum Anwerben von Insidern **55**

Tabelle B.15 — Qualitativer Angriffswert nach Art der vom Angreifer genutzten Ausstattung **55**

Tabelle B.16 — Qualitativer Angriffswert nach Vermeidung von Sichtbarkeit **56**

Tabelle B.17 — Qualitativer Angriffswert nach Mitteln zum Ersatz fehlender Komponenten 57

Tabelle B.18 — Qualitativer Angriffswert nach allgemeinem Angriffswissen..... 58

Tabelle B.19 — Qualitativer Angriffswert nach Verfügbarkeit der Angriffsmethode..... 58

Tabelle B.20 — Qualitativer Angriffswert nach Zeitfenster zum Erreichen der Ziele..... 59

Tabelle B.21 — Qualitativer Angriffswert nach dem für den Angreifer daraus abgeleiteten Wert..... 60

Tabelle B.22 — Qualitativer Angriffswert nach Zielsetzung..... 61

Tabelle B.23 — Qualitativer Angriffswert nach rechtlichen und ethischen Beschränkungen 61

Tabelle B.24 — Qualitativer Angriffswert nach geopolitischem Kontext..... 62

Tabelle B.25 — Zusammenfassung der CTI-Kriterien zur Anwendung in der APL-Bewertung 65

Tabelle B.26 — Methode zur Einschätzung des APL durch Anwendung der für die Anfälligkeitsanalyse relevanten CTI-Merkmale 66

Tabelle C.1 — Anwendungsbeispiel des CSL-Ansatzes — CSL2..... 69

Tabelle C.2 — Anwendungsbeispiel des CSL-Ansatzes — CSL3..... 69

Tabelle C.3 — Anwendungsbeispiel des CSL-Ansatzes — CSL4..... 70

Tabelle C.4 — Anwendungsbeispiel eines CSL-Ansatzes mit mehreren Sicherheitsebenen..... 70