REGULATORIK-WERKSTATT

CRA

Welche Assets hat ein Produkt?

Asset-Taxonomie als Startpunkt für die Beurteilung von Produktcybersicherheitsrisiken nach dem Cyber Resilience Act

© 2026 Dr. Marlen Hofmann · marlen-hofmann.de · Nutzung für interne, nicht-kommerzielle Zwecke gestattet

DIE AUSGANGSFRAGE

Ohne Assets keine Risikobewertung

Wer die Cybersicherheitsrisiken eines Produkts nach dem CRA identifizieren und bewerten will, braucht Transparenz über die Assets, die Cyberbedrohungen ausgesetzt sind. (Vgl. CRA, Art. 13 Abs. 3)

Anhaltspunkte für eine Kategorisierung dieser Assets liefern zwei Entwürfe:

Normentwurf

prEN 40000-1-2, 6.4.2.1

Daten

Funktionen

Soft- und Hardwarekomponenten samt Schnittstellen

Netzwerk und angrenzende Geräte

Vermögenswerte des Nutzers

Vermögenswerte Dritter und der Allgemeinheit

BSI

TR-03183-1, Tab. 1 bis 3

Datenwerte, z. B. personenbezogene Daten, Geschäftsdaten, Telemetrie, Konfigurationsdaten

Funktionswerte, z. B. wesentliche und nicht wesentliche Funktionen, Safety-Funktionen, Kommunikation

Sicherheitswerte, z. B. Geheimnisse, Zertifikate, Sicherheitsprotokolle, Sicherheitsmechanismen

© 2026 Dr. Marlen Hofmann · All rights reserved · Nutzung für interne, nicht-kommerzielle Zwecke gestattet

Den Beispielen einen Rahmen geben

Um eine strukturierte Identifikation und Klassifikation von Assets zu erreichen, ist eine Taxonomie hilfreich, die verschiedene Asset-Klassen festlegt. Weit verbreitet in der Informationssicherheit ist dabei die Einteilung gemäß ISO 27005.

Primäre Assets

- Geschäftsprozesse und -aktivitäten
- Informationen

Unterstützende Assets

- Hardware
- Software
- Netzwerk
- Personal
- Standort
- Organisationsstruktur

Das Problem: Diese Einteilung kommt aus dem Fokus der ISO 27001 auf Unternehmen – im Vordergrund stehen Werte eines Unternehmens –, es muss hier also Anpassungen geben.

Quelle: ISO/IEC 27005:2018, Anhang B.

© 2026 Dr. Marlen Hofmann · All rights reserved · Nutzung für interne, nicht-kommerzielle Zwecke gestattet

Die Taxonomie im Überblick

Die Einteilung der ISO 27005 bleibt, ergänzt um eine dritte Klasse.

CRA (Vorschlag)	
Primäre Assets	Funktionswerte Datenwerte
Unterstützende IKT-Assets	Software · Hardware · Schnittstellen · Netzwerkkomponenten · physische Infrastruktur · IKT-Dienste
Schutzwürdige Interessen	Interessen der Nutzer Interessen Dritter

Neu ist die dritte Zeile: Interessen außerhalb des Produkts werden selbst zu Assets.

© 2026 Dr. Marlen Hofmann · All rights reserved · Nutzung für interne, nicht-kommerzielle Zwecke gestattet

Datenwerte

Datenwerte decken sich fast 1:1 mit den Informationswerten eines Unternehmens gemäß ISO 27005.

Unterart	Was dazugehört	Beispiele
Fachliche Daten	Daten aus den Kern- und Nebenfunktionen	Kontostand, Messwerte, Kennzahlen, geistiges Eigentum
Technische Daten	Konfigurations- und Betriebsdaten	Einstellungen, Telemetrie, Geräte-ID
Sicherheitsdaten	Daten, die Sicherheitsfunktionen brauchen oder erzeugen	API-Schlüssel, Passwörter, Zertifikate, Sicherheitsprotokolle
Personenbezogene Daten	Daten mit Personenbezug, quer zu den übrigen Unterarten	IP-Adressen, Namen, Bilder, Finanz- und Gesundheitsdaten

Beispiele nach BSI TR-03183-1, Tab. 1 und 3.

© 2026 Dr. Marlen Hofmann · All rights reserved · Nutzung für interne, nicht-kommerzielle Zwecke gestattet

Funktionswerte

Funktionswerte entsprechen den Geschäftsprozessen in ISO 27005. Während in der ISO die schützenswerten Prozesse eines Unternehmens erfasst werden, sind unter CRA die schützenswerten Funktionen des Produkts zu erfassen.

Unterart	Beispiele
Fachliche Funktionen z. B. Kern- und Nebenfunktionen	Überweisung, Türöffnen, Aufzeichnen
Technische Funktionen z. B. Kommunikations- und Betriebsfunktionen	Synchronisation, Kopplung mit Geräten in der Nähe, Konfiguration
Sicherheitsfunktionen z. B. Zugangs-, Kryptografie- und Aktualisierungsfunktionen	Anmeldung, Verschlüsselung, Zugriffskontrolle, Update

Beispiele nach BSI TR-03183-1, Tab. 2 und 3.

© 2026 Dr. Marlen Hofmann · All rights reserved · Nutzung für interne, nicht-kommerzielle Zwecke gestattet

Unterstützende IKT-Assets

Dieselben Kategorien wie in der ISO 27005, bezogen auf das Produkt und seine Datenfernverarbeitung.

Unterart	Beispiele
Software	App, Bibliotheken, Firmware
Hardware	Gerät, Chip, Server
Schnittstellen	Programmierschnittstellen, Funk- und Kabelanschlüsse
Netzwerkkomponenten	Router, Gateways, Funkmodule
Physische Infrastruktur	Standorte und Rechenzentren der Datenfernverarbeitung
IKT-Dienste	Backend- und Cloud-Dienste

Die Datenfernverarbeitung gehört zum Produkt, auch wenn ein Dritter sie betreibt (Art. 3 Nr. 2 CRA). Die physische Umgebung des Geräts selbst gehört zum Produktkontext (prEN 40000-1-2, 6.2.3).

© 2026 Dr. Marlen Hofmann · All rights reserved · Nutzung für interne, nicht-kommerzielle Zwecke gestattet

Schutzwürdige Interessen

Eine eigene, dritte Klasse: weder primär noch unterstützend und trotzdem Assets. Anforderungsquellen sind der CRA und der Normentwurf.

Unterart	Was dazugehört
Interessen der Nutzer	Privatsphäre, Leben und Gesundheit, Sicherheit, Vermögen
Interessen Dritter und der Allgemeinheit	Privatsphäre, Leben, Gesundheit und Sicherheit anderer Personen, Eigentum Dritter, Tiere, Umwelt, öffentliches Interesse

Motiviert im CRA

Art. 13 Abs. 2

Auswirkungen von Sicherheitsvorfällen sind so gering wie möglich zu halten, „auch in Bezug auf die Gesundheit und Sicherheit der Nutzer“.

Konkretisiert im Normentwurf

prEN 40000-1-2, 6.4.2.1

Er zählt die Vermögenswerte des Nutzers, Dritter und der Allgemeinheit zu den Assets.

© 2026 Dr. Marlen Hofmann · All rights reserved · Nutzung für interne, nicht-kommerzielle Zwecke gestattet

DER ZUSAMMENHANG

Wie die Klassen zusammenhängen

Risiken werden ermittelt, indem für die Assets die Bedrohungen bestimmt werden, die ein Schutzziel verletzen können (vgl. prEN 40000-1-2). Der Weg einer Bedrohung führt durch alle drei Klassen.

Bedrohung → **trifft ein IKT-Asset** → **verletzt einen Daten- oder Funktionswert** → **schadet einem schutzwürdigen Interesse**

Bedrohung	IKT-Asset	Daten- oder Funktionswert	Schutzwürdiges Interesse
Ausnutzen einer Schwachstelle in einer Bibliothek	Software	Überweisung (Integrität)	Vermögen des Nutzers
Abhören einer unverschlüsselten Verbindung	Schnittstelle	Zugangsdaten (Vertraulichkeit)	Privatsphäre, Vermögen
Ausfall des Cloud-Dienstes	IKT-Dienst	Türöffnen (Verfügbarkeit)	Sicherheit des Nutzers
Übernahme des Geräts für ein Botnetz	Hardware	Kommunikation (Integrität)	Interessen Dritter

Beispiele zur Veranschaulichung, keine abschließende Liste.

© 2026 Dr. Marlen Hofmann · All rights reserved · Nutzung für interne, nicht-kommerzielle Zwecke gestattet

UND JETZT?

Der erste Baustein einer Methode

Die Asset-Taxonomie ist der Ausgangspunkt. Auf ihr bauen die weiteren Schritte einer Methode zur Risikobeurteilung nach dem CRA auf.

1. Produktkontext festlegen
2. Risikoakzeptanzkriterien festlegen
3. **Assets und Cybersicherheitsziele identifizieren** — **dieses Karussell**
4. Bedrohungen identifizieren
5. Wahrscheinlichkeit und Ausmaß abschätzen, Risiken bewerten
6. Risiken behandeln

Weitere Bausteine der Methode folgen. Schritte nach prEN 40000-1-2, Kap. 6.

© 2026 Dr. Marlen Hofmann · marlen-hofmann.de · Nutzung für interne, nicht-kommerzielle Zwecke gestattet