

Welche Produkte von Finanzunternehmen unter den Cyber Resilience Act (CRA) fallen

- Ein Cheatsheet aus der Regulatorik-Werkstatt von Dr. Marlen Hofmann -

DISCLAIMER: Das Cheatsheet dient als Orientierungshilfe für einen ersten Überblick über die Produktkategorien des Cyber Resilience Act (CRA). Es ist nicht rechtsverbindlich und ersetzt keine juristische Prüfung. Die Einstufung setzt voraus, dass das Produkt unter eigenem Namen oder eigener Marke abgegeben wird; die Rolle (Hersteller oder Händler) ist je Konstellation gesondert zu prüfen.

KRITISCHE PRODUKTE CRA Anhang IV	Hardwaregeräte mit Sicherheitsboxen • Bezahlterminals für Händlerkunden — z. B. das Sparkassen-Terminal S-POS Cube	CRA Anh. IV Nr. 1 / DVO 2025/2392 Anh. II Nr. 1 — „Hardwaregeräte mit Sicherheitsboxen“ · explizit genannt: „physische Zahlungsterminals“
	Chipkarten und Sicherheitselemente • Bank- und Zahlungskarten — Debit, Kredit, Prepaid • HBCI-Chipkarten — Zugang zur Zahlungsverkehrs-Software von Firmenkunden • Schließfach-Zutrittskarten • Bezahl-Wearables — Armbänder, Ringe, Schlüsselanhänger • Hardware-Wallets — Verwahrgerät für Krypto-Werte	CRA Anh. IV Nr. 3 / DVO 2025/2392 Anh. II Nr. 3 — „Chipkarten oder ähnliche Geräte, einschließlich Sicherheitselemente“ · explizit genannt: „physische Zahlungskarten“ · „physische Zugangskarten“ · „Armbänder mit integrierten Sicherheitselementen für Zahlungen“ · „Sicherheitselemente, die in Trägermaterialien in anderer Form integriert sind“ Gefertigt von Spezialanbietern. CRA-relevant für das Finanzunternehmen, sobald es sie unter eigenem Namen oder eigener Marke ausgibt: Art. 21 CRA macht den Markenträger zum Hersteller.
WICHTIGE PRODUKTE KLASSE II CRA Anhang III Kl. II	Hypervisoren · Firewalls und Angriffserkennung · manipulationssichere Chips Für Finanzunternehmen mutmaßlich keine eigenen Produkte.	CRA Anh. III Kl. II Nr. 1–4 / DVO 2025/2392 Anh. I Kl. II Nr. 1–4 — „Hypervisoren und Container-Runtime-Systeme ...“ · „Firewalls, Intrusion-Detection-Systeme und Intrusion-Prevention-Systeme“ · „manipulationssichere Mikroprozessoren“ · „manipulationssichere Mikrocontroller“
WICHTIGE PRODUKTE KLASSE I CRA Anhang III Kl. I	Identitätsmanagement und privilegierte Zugriffe • Kartenleser fürs Onlinebanking — chipTAN, photoTAN • TAN-Generatoren und Sicherheitsschlüssel — auch FIDO-Token • TAN- und Freigabe-Apps — pushTAN, SecureGo, Authenticator	CRA Anh. III Kl. I Nr. 1 / DVO 2025/2392 Anh. I Kl. I Nr. 1 — „Identitätsmanagementsysteme sowie Software und Hardware für die Verwaltung privilegierter Zugänge bzw. Zugriffe, einschließlich Lesegeräte für die Authentifizierung und Zugangskontrolle, auch biometrische Lesegeräte“ · explizit genannt: „Lesegeräte für die Authentifizierung und Zugangskontrolle“ · „Hardware-Authentifizierungsgeräte wie Generatoren für Transaktionsnummern (TAN-Generatoren)“ · „Authentifizierungssoftware und Multi-Faktor-Authentifizierungssoftware“ Gefertigt von Spezialanbietern. CRA-relevant, sobald das Finanzunternehmen sie unter eigenem Namen oder eigener Marke ausgibt (Art. 21 CRA).
STANDARD- PRODUKTE Art. 2 Abs. 1 CRA	Apps für Endkunden • Banking- und Trading-Apps • Krypto-Wallet-Apps — Selbstverwahrung durch den Kunden • Crowdfunding-Apps — Anlegerzugang der Plattformen • Browser-Erweiterungen — Banking-Plugin, Wallet-Erweiterung • Smartphone als Kartenterminal — SoftPOS-App für Händlerkunden	Art. 2 Abs. 1 CRA — erfasst sind Produkte mit digitalen Elementen, „deren bestimmungsgemäßer Zweck oder vernünftigerweise vorhersehbare Verwendung eine direkte oder indirekte logische oder physische Datenverbindung mit einem Gerät oder Netz einschließt“
	Software für Firmenkunden und Partner • Zahlungsverkehrs-Software — EBICS-Client • Bezahl-Bausteine für Partner — Bezahlfunktion, die ein Online-Shop einbaut • Börsen-Handelssoftware — Oberfläche für Börsenteilnehmer • Excel-Zusatzprogramme — Marktdaten- und Rating-Add-ins Geräte und Karten • Versichertenkarten — Chipkarte der privaten Krankenversicherung; als Speicherchip Standard, als Sicherheitselement wäre sie kritisch • Telematik-Boxen der Kfz-Versicherer — Sensor im Fahrzeug beim Telematik-Tarif	Entscheidend ist, wo die Software läuft: Was der Nutzer ausschließlich im Browser aufruft, läuft auf dem Server des Anbieters und ist kein Produkt. Als installierter Client auf dem Gerät des Nutzers ist es eines — deshalb sind Banking-Apps und EBICS-Clients erfasst, das Online-Banking im Browser nicht (Leitlinien Rn. 21, Beispiel 5).
PRODUKTE ANDERER HERSTELLER	Zugekaufte Hardware und Software Geldautomaten und SB-Terminals, Kernbanksystem und Fachanwendungen, SIEM, Firewalls, Betriebssysteme, Cloud-Dienste — sowie alle zugekauften wichtigen und kritischen Produkte der Klassen darüber.	CRA gilt — beim Lieferanten: Herstellerpflichten treffen den Anbieter, nicht das Finanzunternehmen. Hier liegt der Hebel im IKT-Drittparteienrisikomanagement: CRA-Konformität der Lieferanten ist zu prüfen und gegebenenfalls auch vertraglich zu verankern.
PRODUKTE UND SERVICES AUSSERHALB DES CRA kein Produkt mit digitalen Elementen	Web-Anwendungen und Portale Online-Banking im Browser, Bank- und Versicherungs-Websites, Kunden- und Maklerportale, Antrags-, Vergleichs- und Vertragsportale, Schadenmeldung im Browser, PSD2-Schnittstellen und Server-APIs. Dienstleistungen und Daten Zahlungsdienst und Kartenakzeptanz, Verwahrung und Depotführung, Vermittlung und Beratung, Schadenregulierung, Rating und Indexberechnung, Kursfeeds und Meldedaten.	Leitlinien Rn. 21, Beispiele 5 und 6: Web-Anwendungen und Websites sind keine Produkte mit digitalen Elementen Art. 3 Nr. 1 CRA: weder Hard- noch Software — keine Produkte im Sinne der Verordnung