IVRSA
INDUSTRIEVEREINIGUNG
Rollladen-Sonnenschutz-Automation

FACH–INFORMATION

FI.02

Cyber Resilience Act (CRA)
Praxishinweise für Hersteller von Sonnenschutz-, Antriebs- und Smart-Home-Systemen

Stand September 2026

Der **Cyber Resilience Act (CRA)** ist die EU-Verordnung 2024/2847 und schafft erstmals verbindliche Cybersicherheitsanforderungen für Produkte mit digitalen Elementen, also für Hard- und Softwareprodukte, die direkt oder indirekt mit einem Gerät oder Netzwerk verbunden sind. Wer Produkte mit digitaler Funktion und EU-Marktzugang anbietet, muss prüfen, ob die Produkte in den Anwendungsbereich fallen, wie sie einzustufen sind und welche technischen, organisatorischen und dokumentarischen Pflichten daraus folgen. Typische Funktionen sind Funkbedienung, App-Steuerung, Cloud-Zugriff, Sprachassistenten-Anbindung, automatische Fahrbefehle, Zeitprogramme, Wetterstationen, Szenarien sowie die Integration in KNX-, Matter-, Zigbee-, Z-Wave-, WLAN- oder proprietäre Systeme. Unautorisierte Steuerbefehle, unsichere Firmware-Updates, schwache Authentisierung, unsichere APIs oder angreifbare mobile Apps können die Produktsicherheit beeinträchtigen. Der CRA adressiert genau diese Risiken. Ziel ist, dass Produkte bereits beim Inverkehrbringen ein Mindestniveau an Cybersicherheit aufweisen und während ihres gesamten Supportzeitraums sicher gehalten werden. Die Verordnung verlangt also nicht nur sichere Produktentwicklung, sondern auch ein funktionierendes Schwachstellenmanagement, Sicherheitsupdates und Meldeprozesse für aktiv ausgenutzte Schwachstellen und schwere Sicherheitsvorfälle.

Die Verordnung gilt gestuft: in Kraft seit 10.12.2024, Meldepflichten ab 11.09.2026, vollständige Geltung ab 11.12.2027.

Welche Produkte sind betroffen?

- Funkmotoren und elektronische Antriebe mit digitaler Steuerlogik.
- Wandsteuerungen, Handsender, Smart-Home-Bridges und Gateways mit Netzwerk- oder Cloud-Anbindung.
- Smartphone-Apps und Webportale zur Steuerung von Sonnenschutzanlagen.
- Zentrale Steuergeräte für Rollladen-, Markisen- und Raffstoresysteme in Wohn- und Zweckbauten.
- Sensorik mit digitaler Kommunikation, etwa Wetterstationen, Wind-, Sonnen- oder Temperatursensoren mit Bus- oder Funkanbindung
- Produkte mit Integrationen zu Sprachassistenten oder Smart-Home-Ökosystemen.

Nicht entscheidend ist, ob ein Produkt „IT“ im klassischen Sinn ist. Entscheidend ist, ob es ein Produkt mit digitalen Elementen ist und auf dem EU-Markt bereitgestellt wird.

Entscheidend ist dabei nicht, ob ein Produkt über eine Internetverbindung erreichbar ist. Der CRA setzt eine direkte oder indirekte, logische oder physische Datenverbindung zu einem Gerät oder Netz voraus; eine Funkverbindung zu einem anderen Gerät genügt. Auch unidirektionale Funkstrecken (etwa zwischen Handsender und Antrieb) begründen regelmäßig eine logische Datenverbindung und führen damit nicht aus dem Anwendungsbereich heraus. Rein mechanische Produkte ohne jede Datenverbindung fallen dagegen nicht unter den CRA. Gleiches gilt für Antriebe, die ausschließlich über einen konventionellen Schalter angesteuert werden.

Zu beachten ist außerdem die Rollenfrage: Wer ein Produkt unter eigenem Namen oder eigener Marke in Verkehr bringt oder es wesentlich verändert, gilt als Hersteller im Sinne des CRA mit allen Herstellerpflichten. Auch bei zugekauften Antrieben, Funkmodulen oder Gateways. Private-Label- und OEM-Konstellationen sind daher je Produkt eindeutig zuzuordnen.

Bei zusammengesetzten Anlagen ist die Rolle für jede Komponente getrennt zu bestimmen. Wer einen Antrieb, eine Steuerung, einen Sensor oder einen Handsender selbst in Verkehr bringt, trägt dafür die Herstellerpflichten.
Wird eine solche Komponente in eine Anlage eingebaut, entsteht ein eigenes Produkt mit digitalen Elementen, für das derjenige verantwortlich ist, der die Anlage in Verkehr bringt. Zugekaufte Bauteile mit eigenem CE entbinden davon nicht. Wird eine Komponente dagegen unverändert in der Originalverpackung mit Typenschild und Konformitätserklärung des Komponentenherstellers weitergegeben, greifen nur die schlankeren Händlerpflichten.

Achtung! Meldepflichten ab 11. September 2026

Hersteller müssen aktiv ausgenutzte Schwachstellen und schwere Sicherheitsvorfälle melden, wenn diese die Sicherheit eines Produkts mit digitalen Elementen betreffen. Die Meldekette ist gestuft:

- Frühwarnung innerhalb von 24 Stunden nach Bekanntwerden.
- Vollständige Meldung innerhalb von 72 Stunden.
- Abschlussbericht bei Schwachstellen spätestens 14 Tage nach Verfügbarkeit einer Korrekturmaßnahme; bei schweren Sicherheitsvorfällen innerhalb eines Monats nach der 72-Stunden-Meldung.

Wichtig: Die Meldepflicht gilt auch für Bestandsprodukte

Die Meldepflichten gelten ab 11.09.2026 für alle Produkte im Anwendungsbereich, die vor dem 11.12.2027 in Verkehr gebracht wurden, unabhängig davon, ob sie jemals verändert werden. Antriebe, Sensoren, Steuerzentralen und Apps, die seit Jahren im Feld sind, sind erfasst.

Melden: ja.
Zu melden sind aktiv ausgenutzte Schwachstellen und schwere Sicherheitsvorfälle, nicht aber jede kleine Lücke. Eine Schwachstelle, die niemand ausnutzt, löst keine Behörden-meldung aus.

Patchen: nein.
Die Pflicht zum Schwachstellenmanagement gehört zu den Anforderungen, von denen Bestandsprodukte freigestellt sind. Aus dem CRA folgt für ein Altprodukt keine Pflicht, einen Patch zu entwickeln.

Nutzer informieren: ja.
Betroffene Nutzer sind über die Schwachstelle und über erforderliche Abhilfemaßnahmen zu unterrichten. Ist kein Update möglich, muss informiert werden, was der Nutzer stattdessen tun soll. Etwa Deaktivierung einer Funktion oder Austausch der Komponente.

Die Meldung erfolgt grundsätzlich nur einmal über die CRA Single Reporting Plattform an das zuständige nationale CSIRT und zugleich an ENISA.

Zusätzlich zur Behördenmeldung sind die betroffenen Nutzer unverzüglich über die Schwachstelle oder den Vorfall und über erforderliche Abhilfemaßnahmen zu informieren. Betrifft die Schwachstelle eine zugekaufte Komponente, ist auch deren Anbieter zu unterrichten. Die Fristen laufen ab Kenntnisnahme, also auch an Wochenenden.

Für Hersteller bedeutet das praktisch, dass sie spätestens jetzt interne Prozesse brauchen, um Schwachstellenbewertung, Eskalation, Freigabe und Meldung rund um die Uhr oder zumindest mit klar definierten Verantwortlichkeiten sicherzustellen.

Was Unternehmen bis Dezember 2027 grundsätzlich erfüllen müssen

Der CRA verlangt, dass Hersteller Cybersicherheit über den gesamten Produktlebenszyklus berücksichtigen. Dazu gehören Planung, Design, Entwicklung, Produktion, Inverkehrbringen, Support und Schwachstellenbehandlung. Die folgenden Pflichten sind für die Praxis besonders wichtig.

Produktklassifizierung und Scope-Prüfung

Unternehmen sollten jedes relevante Produktportfolio zunächst systematisch prüfen: Fällt das Produkt unter den CRA, ist es Standard-, wichtiges oder kritisches Produkt, und welche Konformitätsbewertung ist erforderlich?

Produkte mit Sicherheitsfunktionen im Smart-Home-Bereich können einer strengeren Betrachtung unterliegen. Der CRA nennt unter anderem Smart-Home-Produkte mit Sicherheitsfunktionen wie smarte Türschlösser, Sicherheitskameras, Baby-Monitore und Alarmanlagen als wichtige Produkte mit digitalen Elementen. Auch wenn motorisierte Sonnenschutzsysteme nicht automatisch in diese Kategorie fallen, kann eine ähnliche Risikologik relevant werden, etwa wenn Produkte Zutritts-, Schutz- oder Sicherheitsfunktionen beeinflussen.

Nach derzeitiger Einschätzung sind Sonnenschutzsteuerungen und motorisierte Sonnenschutzsysteme in aller Regel Standardprodukte, für die eine Selbstbewertung (interne Kontrolle) genügt. Die Einstufung ist zu dokumentieren.

Abgrenzung zur Funkanlagenrichtlinie (RED) und EN 18031

Für internetfähige Funkanlagen gelten die Cybersicherheitsanforderungen der RED (Radio Equipment Directive) bereits seit 1. August 2025. Harmonisierte Normen sind EN 18031-1, EN 18031-2 und EN 18031-3.
Diese Anforderungen greifen also heute schon und werden häufig mit dem CRA verwechselt. Der CRA tritt ab 11.12.2027 hinzu, gilt auch für nicht funkbasierte Produkte und begründet zusätzlich Prozess- und Meldepflichten. Für motorisierte Systeme ist zudem die Maschinenverordnung ab 20.01.2027 zu beachten. Für reine Funkprodukte ohne Internetanbindung greift damit erst der CRA ab 11.12.2027. Sobald ein Gateway mit Internetanbindung Teil der Anlage ist, kann die RED bereits heute einschlägig sein; diese Abgrenzung ist im Einzelfall zu prüfen.

Secure by Design und Secure by Default

Produkte müssen so gestaltet sein, dass sie ein angemessenes Sicherheitsniveau aufweisen und mit sicheren Voreinstellungen ausgeliefert werden. Praktisch bedeutet das zum Beispiel:

- Keine universellen Standardpasswörter im Feldbetrieb.
- Sichere Erstinbetriebnahme mit erzwungener Individualisierung von Zugangsdaten, wo Authentisierung erforderlich ist.
- Deaktivierte unsichere oder nicht benötigte Dienste im Auslieferungszustand.
- Minimierung offener Ports, Dienste und Schnittstellen.
- Rücksetzfunktion auf einen definierten sicheren Ausgangszustand.

Für Antriebs- und Steuerungshersteller heißt das konkret: Eine App-fähige Steuerzentrale sollte nicht mit allgemein bekannten Standard-Zugangsdaten ausgeliefert werden. Ein Funkgateway sollte nicht ungeschützt im lokalen Netz erreichbar sein. Eine Cloud-Anbindung sollte standardmäßig mit sicherer Transportverschlüsselung und sauberem Authentisierungsmodell arbeiten.

Risikoanalyse und technische Sicherheitsanforderungen
Hersteller müssen die Cybersicherheitsrisiken ihrer Produkte dokumentiert bewerten und daraus Schutzmaßnahmen ableiten. Diese Risikoanalyse sollte mindestens folgende technische Ebenen umfassen:

- Hardware und physische Schnittstellen, etwa Debug-Ports oder ungeschützte Serviceanschlüsse
- Firmware und Boot-Prozess, etwa Secure Boot, Signaturprüfung und Schutz vor Manipulation
- Kommunikationsschnittstellen wie WLAN, Bluetooth, Zigbee, Thread, KNX IP, Matter-Bridges oder proprietäre Funkprotokolle.
- Mobile Apps, Backends, Webportale und Cloud-Schnittstellen.
- Benutzer- und Rechtekonzepte für Installateure, Endkunden, Administratoren und Servicepartner

Leitfragen für die Risikoanalyse

- Kann ein Angreifer einen Motor über das Netzwerk unautorisiert ansteuern?
- Ist die Funkkommunikation gegen Replay-Angriffe geschützt?
- Lassen sich Firmware-Dateien manipulieren?
- Können OAuth-, API- oder App-Token abgegriffen oder missbraucht werden?
- Sind lokale Fallback-Modi sicher gestaltet?

Schwachstellenmanagement und Security Updates
Der CRA verlangt ein strukturiertes Vulnerability Handling über den gesamten Supportzeitraum des Produkts. Unternehmen müssen Schwachstellen aufnehmen, bewerten, priorisieren, beheben und Sicherheitsupdates bereitstellen. Updates sollen sicher verteilt werden; wo angemessen, sollen Sicherheitsupdates automatisch oder mit standardmäßig aktivierter Updatefunktion bereitgestellt werden, mit transparenter Opt-out- oder Aufschubmöglichkeit.

Für die Praxis bedeutet das:

- Einrichtung einer zentralen Vulnerability-Management-Funktion.
- Veröffentlichung einer Kontaktstelle und einer Policy zur koordinierten Offenlegung von Schwachstellen.
- Klare Trennung von Security-Updates und Funktionsupdates, soweit technisch sinnvoll.
- Kryptografisch gesicherte Update-Pakete mit Integritäts- und Authentizitätsprüfung.
- Updatefähigkeit auch für Bestandsprodukte, soweit vom Supportzeitraum umfasst.

Ein Beispiel: Wenn eine Smart-Home-Zentrale für Rollläden eine Sicherheitslücke in ihrer Weboberfläche hat, muss der Hersteller nicht nur den Patch entwickeln, sondern auch einen verlässlichen Verteilmechanismus, ein Test- und Freigabeverfahren, Kundeninformation und gegebenenfalls die CRA-Meldepflichten organisieren, falls die Lücke aktiv ausgenutzt wird.

Unterstützungszeitraum und Produktpflege
Hersteller müssen einen Unterstützungszeitraum definieren, während dessen Schwachstellen behandelt und Sicherheitsupdates kostenlos bereitgestellt werden.
Dies ist keine Empfehlung, sondern Pflicht: Der Unterstützungszeitraum muss die voraussichtliche Nutzungsdauer des Produkts widerspiegeln und beträgt mindestens fünf Jahre; nur wenn das Produkt voraussichtlich kürzer im Betrieb ist, entspricht er dieser kürzeren Nutzungsdauer.
Für langlebige Produkte der Gebäudeautomation ist das besonders relevant, weil Antriebe, Steuerzentralen und Gateways oft deutlich länger als typische Consumer-Elektronik im Markt und im Betrieb bleiben. Die fünf Jahre sind für die Branche daher die Untergrenze, nicht der Zielwert. Die Erwägungen zur Festlegung gehören in die technische Dokumentation, das Ende des Unterstützungszeitraums ist dem Nutzer mitzuteilen, und die Patch-Zusagen der Zulieferer müssen den eigenen Unterstützungszeitraum abdecken.

Technische Dokumentation, CE-Kennzeichnung und Konformität
Konforme Produkte tragen die CE-Kennzeichnung; dafür müssen Hersteller die einschlägigen CRA-Anforderungen erfüllen, die Konformitätsbewertung durchführen und technische Dokumentation vorhalten. Diese Dokumentation sollte unter anderem Risikoanalyse, Sicherheitsarchitektur, verwendete Komponenten, Update-Konzept, Supportzeitraum, Testnachweise und Informationen zur Schwachstellenbehandlung enthalten.

Für Produkte mit höherem Risiko oder bestimmter Klassifizierung kann eine Prüfung durch eine notifizierte Stelle erforderlich werden. Unternehmen sollten deshalb früh prüfen, ob ihre Produktkategorien in Annex III oder IV fallen oder ob harmonisierte Standards verfügbar sind, auf die sie sich stützen können.

Zu beachten ist der Zeitpunkt des Inverkehrbringens: Er bezieht sich auf das einzelne Produktexemplar, nicht auf die Baureihe. Ware, die erst nach dem 11.12.2027 ausgeliefert wird, muss CRA-konform sein, unabhängig davon, wann sie produziert wurde. Lagerreichweiten und auslaufende Produktserien sind entsprechend zu planen.

SBOM und Lieferkette
Die Software Bill of Materials (SBOM) ist eine unmittelbare Rechtspflicht aus Anhang I Teil II Nr. 1 CRA: Komponenten und Schwachstellen sind zu erfassen und zu dokumentieren, einschließlich einer SBOM in einem gängigen maschinenlesbaren Format, das mindestens die Top-Level-Abhängigkeiten abdeckt. Die BSI-Richtlinie TR-03183 konkretisiert die Anforderungen, ist aber Auslegungshilfe und nicht Rechtsgrundlage.

Für Hersteller vernetzter Steuerungen und Apps ist das praktisch wichtig, weil viele Sicherheitslücken nicht im eigenen Code, sondern in eingebetteten Open-Source- oder Drittkomponenten entstehen.

Eine gepflegte SBOM hilft dabei, betroffene Produkte bei Sicherheitsmeldungen schnell zu identifizieren. Das ist besonders relevant, wenn mehrere Produktgenerationen dieselben Bibliotheken, Funkmodule, Chipsätze, Linux-Komponenten, mobile SDKs oder Cloud-Bausteine einsetzen. Ergänzend verlangt der CRA die gebotene Sorgfalt bei der Integration von Komponenten Dritter.

Sanktionen
Verstöße gegen die grundlegenden Anforderungen nach Anhang I sowie gegen die Pflichten aus Art. 13 und Art. 14 können mit Geldbußen bis zu 15 Mio. EUR oder 2,5 % des weltweiten Jahresumsatzes geahndet werden, je nachdem, welcher Betrag höher ist; für sonstige Pflichtverstöße gelten bis zu 10 Mio. EUR oder 2 %. Größenbezogene Ausnahmen für KMU bestehen nicht.

Konkrete Maßnahmen zur technischen Umsetzung

Governance und Organisation
- CRA-Verantwortung im Unternehmen festlegen, idealerweise mit Schnittstelle zwischen Entwicklung, IT-Security, Qualität, Produktmanagement und Recht.
- Meldeprozess für Art.-14-Fälle definieren, inklusive 24h-/72h-/14-Tage-Ablauf.
- Incident-Response- und Vulnerability-Disclosure-Prozess etablieren.
- Bestandsaufnahme aller Produkte mit digitalen Elementen erstellen, einschließlich Bestandsprodukten im Feld.
- Je Produkt festlegen, wer CRA-Hersteller ist (Eigenentwicklung, OEM, Private Label).

Entwicklung und Architektur
- Secure Development Lifecycle einführen oder schärfen.
- Threat Modeling für Gateways, Apps, Funkstrecken, APIs und Cloud-Komponenten durchführen.
- Sichere Update-Architektur mit Signierung, Rollback-Schutz und Authentizitätsprüfung umsetzen.
- Starke Authentisierung und Rechtekonzepte für Service- und Installateurzugänge definieren.
- Logging und Ereignisprotokollierung für sicherheitsrelevante Aktionen vorsehen, soweit technisch und datenschutzrechtlich angemessen.

Test und Qualitätssicherung
- Security-Tests in den Entwicklungsprozess integrieren, zum Beispiel statische Codeanalyse, Penetrationstests, API-Tests, Funkprotokolltests und Update-Tests.
- Prüfung auf bekannte Schwachstellen in Drittbibliotheken automatisieren.
- Härtungstests für Default-Konfigurationen und Ersteinrichtung durchführen.

Betrieb und Support
- Security-Advisory-Prozess aufbauen.
- Unterstützungszeitraum und Update-Politik transparent veröffentlichen.
- Prozesse für Bestandskundenkommunikation, Rückrufe, Hotfixes und sichere Migration etablieren.

Empfohlener Maßnahmenplan für Mitgliedsunternehmen

Sofort
- Produktportfolio auf CRA-Relevanz prüfen.
- Verantwortliche Person oder Taskforce benennen.
- Meldestruktur für aktiv ausgenutzte Schwachstellen und schwere Vorfälle festlegen.
- Kontaktkanal für Vulnerability Disclosure einrichten.
- Zugang zur Meldeplattform und zuständiges CSIRT klären, Ersatzmeldeweg dokumentieren, Meldeprozess testen.

In den nächsten 3 bis 6 Monaten
- Risikoanalyse für Kernprodukte durchführen.
- Update- und Supportkonzept definieren.
- Sicherheitsanforderungen in Lastenhefte und Entwicklungsprozesse integrieren.
- SBOM-Prozess und Komponenteninventar aufbauen.
- Unterstützungszeiträume je Produkt festlegen und Patch-Zusagen der Lieferanten prüfen.

Bis zur vollen Geltung
- Technische Dokumentation CRA-fähig machen.
- Konformitätsbewertung vorbereiten.
- Security-Tests und Freigabeprozesse standardisieren.
- Kunden- und Marktkommunikation zu Supportzeiten und Updates professionalisieren.
- Lagerreichweiten und Auslaufserien im Hinblick auf den 11.12.2027 bewerten.

Weitere Richtlinien, Leitfäden, Merkblätter finden Sie unter folgendem QR-Code

IVRSA
INDUSTRIEVEREINIGUNG
Rollladen-Sonnenschutz-Automation

Industrievereinigung
Rollladen-Sonnenschutz-
Automation e.V.
Heinrichstraße 79
D-36037 Fulda
Telefon: 0661 90 19 60 11
Telefax: 0661 90 19 63 20

Homepage: www.ivrsa.de
E-Mail: info@ivrsa.de