SE

EMBEDDED SYSTEMS ENGINEERING

SCHMITT CONSULTING S.A.R.L. · SC-SARL.COM

CRA-snelcheck voor apparaatfabrikanten

De nieuwe EU-wet over de cyberbeveiliging van verbonden producten — wat vóór september 2026 op orde moet zijn, in begrijpelijke taal.

Eerste bindende deadline: 11 september 2026

Niet pas 2027. Wie zich nu niet voorbereidt, komt in tijdnood.

1 Waar het om gaat

De **Cyber Resilience Act** — kortweg **CRA** — is sinds december 2024 van kracht. Hij schrijft voor hoe veilig verbonden producten moeten zijn tegen aanvallen vanaf het internet. Het betreft alles wat software bevat of verbinding maakt met een netwerk: van de slimme thermostaat tot industriële besturingen en de app.

Veel fabrikanten denken tot eind 2027 de tijd te hebben. Dat geldt slechts voor een deel van de verplichtingen. De **eerste bindende deadline ligt al in september 2026** — en geldt ook voor producten die allang op de markt zijn en nog worden onderhouden.

11 september 2026

Meldplicht. Wordt een kwetsbaarheid aantoonbaar door aanvallers misbruikt, dan moet dat **binnen 24 uur** bij de autoriteiten worden gemeld.

11 december 2027

Alle overige verplichtingen. Product veilig vanaf het ontwerp, beveiligingsupdates gedurende de hele levensduur, volledige software-stuklijst, formele beoordeling en CE-markering.

De mogelijke boetes lopen op tot **15 miljoen euro of 2,5 % van de wereldwijde jaaromzet** — afhankelijk van welk bedrag hoger is. En: de wet geldt uitdrukkelijk ook voor kleine fabrikanten en eenmansaanbieders, niet alleen voor grote concerns.

2 De belangrijkste begrippen — kort uitgelegd

Firmware

De vast in een apparaat ingebouwde besturingssoftware die ervoor zorgt dat het überhaupt werkt — bijvoorbeeld de programmacode in een machine, een sensor of een besturing.

Kwetsbaarheid (zwakke plek)

Een fout of zwakte in de software waarmee een aanvaller in het apparaat kan binnendringen of het kan manipuleren.

Software-stuklijst (SBOM)

Een volledige lijst van alle softwarecomponenten van een product — vergelijkbaar met de stuklijst van een onderdeel, maar dan voor de programmacode. Zonder die lijst valt niet te zeggen of het product door een bekende kwetsbaarheid wordt getroffen.

ENISA / CSIRT

ENISA is het EU-agentschap voor cyberbeveiliging, het centrale orgaan voor IT-beveiliging in Europa. CSIRT's zijn de nationale «computer-brandweerkorpsen» die bij beveiligingsincidenten coördineren. Naar hen gaat de melding binnen 24 uur.

Functionele veiligheid

De bescherming van een apparaat tegen technische *storingen en uitval* — gevestigde praktijk in bijvoorbeeld de auto-industrie. De CRA vult dit aan met bescherming tegen *opzettelijke aanvallen*.

CE-markering

De bekende CE-markering op producten. Ze bevestigt dat een product aan de EU-eisen voldoet en op de Europese markt mag worden verkocht.

3 Bent u CRA-klaar? De checklist

Loop de volgende punten na. Elk vakje dat u **niet** met een gerust hart kunt aanvinken, is openstaand werk tot september 2026.

OVERZICHT & ORGANISATIE

- [ ] We weten welke van onze producten onder de wet vallen.
- [ ] We weten welke oudere producten we nog onderhouden (en die dus eveneens worden geraakt).
- [ ] Er is een verantwoordelijke persoon voor het onderwerp CRA binnen het bedrijf.

SOFTWARE-STUKLIJST

- [ ] Voor elk product bestaat een volledige lijst van alle ingebouwde softwarecomponenten.
- [ ] We herkennen daarin ook verouderde bouwstenen die de leverancier niet meer onderhoudt.
- [ ] Deze lijst wordt doorlopend actueel gehouden, niet eenmalig opgesteld.

MELDPROCES (VERPLICHT VANAF 09/2026)

- [ ] Het is geregeld wie een misbruikte kwetsbaarheid opmerkt.
- [ ] Het is geregeld wie ze beoordeelt en wie ze meldt.
- [ ] We kunnen de 24-uurstermijn organisatorisch daadwerkelijk halen — ook in het weekend.

TECHNISCHE BEVEILIGING VAN HET APPARAAT

- [ ] De software in het apparaat is versleuteld opgeslagen en kan niet zomaar worden uitgelezen.
- [ ] Updates zijn fraudebestendig — niemand kan ongemerkt ondergeschoven software installeren.
- [ ] Het apparaat kan gedurende zijn hele levensduur beveiligingsupdates ontvangen.
- [ ] Bij het opstarten controleert het apparaat dat alleen echte, ongewijzigde software draait.

BEWIJS & DOCUMENTATIE

- [ ] We kunnen aantonen dat is ontwikkeld volgens erkende programmeerstandaarden.
- [ ] Storingsbestendigheid en aanvalsbestendigheid worden in één gezamenlijk concept gedacht, niet apart.
- [ ] De documenten die nodig zijn voor de latere conformiteitsbeoordeling worden vanaf het begin bijgehouden.

4 Hoe het verdergaat

De komende maanden beslissen of er in september 2026 een ordelijk proces staat of dat er haastig moet worden geïmproviseerd. Wie vroeg begint, verdeelt het werk — en vermijdt dure noodgrepen vlak voor de deadline. De grootste hefboom ligt meestal niet in de techniek alleen, maar in het goede samenspel van stuklijst, meldproces en apparaatbeveiliging.

→ Verder verdiepen & ondersteuning

Wilt u de eisen niet alleen overzien, maar ook invoeren? Drie wegen:

Vakboeken & software

Praktijkkennis uit meer dan 35 jaar embedded ontwikkeling — de technische basis achter de CRA-eisen. Te vinden op **sc-sarl.com/nl/produkte.html**

Gratis erbij: «Formuleverzameling voor informatici en ingenieurs»

Interactieve HTML-formuleverzameling, 56 hoofdstukken, tweetalig DE/EN, offline bruikbaar — gratis in de downloadsectie.

Persoonlijke ondersteuning

Van de software-stuklijst tot het harden van de firmware. Adviesgesprek op **sc-sarl.com/nl/kontakt.html**

Naar de producten & downloads →