



EMBEDDED SYSTEMS ENGINEERING

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

CRA-hurtigtjek for enhedsproducenter

Den nye EU-lov om cybersikkerhed for forbundne produkter — hvad der skal være på plads inden september 2026, i et forståeligt sprog.

Første bindende frist: 11. september 2026

Ikke først i 2027. Den, der ikke forbereder sig nu, kommer i tidsnød.

1 Hvad det handler om

Cyber Resilience Act — kort **CRA** — har været gældende siden december 2024. Den fastlægger, hvor sikre forbundne produkter skal være mod angreb fra internettet. Den omfatter alt, der indeholder software eller forbinder sig til et netværk: fra den smarte termostat over industristyringer til app'en.

Mange producenter tror, de har tid til udgangen af 2027. Det gælder kun for en del af forpligtelserne. Den **første bindende frist ligger allerede i september 2026** — og den omfatter også produkter, der for længst er på markedet og stadig vedligeholdes.

11. september 2026

Indberetningspligt. Hvis en sårbarhed påviseligt udnyttes af angribere, skal det inden for **24 timer** indberettes til myndighederne.

11. december 2027

Alle øvrige forpligtelser. Produkt sikkert fra bunden, sikkerhedsopdateringer i hele levetiden, fuldstændig software-stykliste, formel vurdering og CE-mærkning.

De mulige bøder når op til **15 millioner euro eller 2,5 % af den globale årsomsætning** — alt efter hvilket beløb der er højest. Og: loven gælder udtrykkeligt også for små producenter og enkeltudbydere, ikke kun for store koncerner.

2 De vigtigste begreber — kort forklaret

Firmware

Den fast indbyggede styringssoftware i en enhed, der får den til at fungere — for eksempel programkoden i en maskine, en sensor eller en styring.

Sårbarhed (sikkerhedshul)

En fejl eller svaghed i softwaren, som en angriber kan trænge ind i enheden gennem eller manipulere den med.

Software-stykliste (SBOM)

En fuldstændig liste over alle softwarekomponenter i et produkt — sammenlignelig med styklisten for en komponent, blot for programkoden. Uden den kan man ikke sige, om produktet er berørt af et kendt sikkerhedshul.

ENISA / CSIRT

ENISA er EU's cybersikkerhedsagentur, det centrale organ for it-sikkerhed i Europa. CSIRT'er er de nationale statslige «computer-brandvæsener», der koordinerer ved sikkerhedshændelser. Til dem går 24-timers-indberetningen.

Funktionel sikkerhed

Beskyttelsen af en enhed mod tekniske *fejlfunktioner og nedbrud* — etableret praksis blandt andet i bilteknik. CRA supplerer dette med beskyttelse mod *bevidste angreb*.

CE-mærkning

Den velkendte CE-mærkning på produkter. Den bekræfter, at et produkt opfylder EU-kravene og må sælges på det europæiske marked.

3 Er I CRA-klar? Tjeklisten

Gennemgå de følgende punkter. Hvert felt, I **ikke** med god samvittighed kan sætte flueben ved, er en åben byggeplads frem til september 2026.

OVERBLIK & ORGANISATION

- Vi ved, hvilke af vores produkter der er omfattet af loven.
- Vi ved, hvilke ældre produkter vi stadig vedligeholder (og som dermed også er omfattet).
- Der er en ansvarlig person for emnet CRA i virksomheden.

SOFTWARE-STYKLISTE

- For hvert produkt findes en fuldstændig liste over alle indbyggede softwarekomponenter.
- Heri genkender vi også forældede komponenter, som leverandøren ikke længere vedligeholder.
- Denne liste holdes løbende ajour, ikke kun udarbejdet én gang.

INDBERETNINGSPROCES (PLIGT FRA 09/2026)

- Det er fastlagt, hvem der bemærker en udnyttet sårbarhed.
- Det er fastlagt, hvem der vurderer den, og hvem der indberetter den.
- Vi kan organisatorisk reelt overholde 24-timers-fristen — også i weekenden.

TEKNISK BESKYTTELSE AF ENHEDEN

- Softwaren i enheden er krypteret lagret og kan ikke uden videre læses ud.
- Opdateringer er forfalskningssikre — ingen kan indsætte software, der er smuglet ind.
- Enheden kan modtage sikkerhedsopdateringer i hele sin levetid.
- Ved opstart kontrollerer enheden, at kun ægte, uændret software kører.

DOKUMENTATION & BEVISER

- Vi kan dokumentere, at der er udviklet efter anerkendte programmeringsstandarder.
- Driftssikkerhed og angrebssikkerhed tænkes i ét fælles koncept, ikke adskilt.
- De dokumenter, der er nødvendige for den senere overensstemmelsesvurdering, føres med fra begyndelsen.

4 Sådan kommer I videre

De kommende måneder afgør, om der i september 2026 står et velordnet forløb, eller om der skal improviseres i hast. Den, der begynder tidligt, fordeler arbejdet — og undgår dyre hovsaløsninger lige før fristen. Den største løftestang ligger som regel ikke i teknikken alene, men i det rene samspil mellem stykliste, indberetningsproces og enhedsbeskyttelse.

→ Gå i dybden & support

Vil I ikke kun have overblik over kravene, men også føre dem ud i livet? Tre veje:

Fagbøger & software

Praktisk viden fra over 35 års embedded-udvikling — det tekniske fundament bag CRA-kravene. Findes på sc-sarl.com/da/produkte.html

Gratis med: «Formelsamling for dataloger og ingeniører»

Interaktiv HTML-formelsamling, 56 kapitler, tosproget DE/EN, kan bruges offline — gratis i downloadområdet.

Personlig støtte

Fra software-styklisten til hærdning af firmwaren. Rådgivningssamtale på sc-sarl.com/da/kontakt.html

[Til produkter & downloads →](#)

Denne vejledning giver et praktisk overblik og erstatter ikke juridisk rådgivning. Afgørende er forordning (EU) 2024/2847. Fristernes status: indberetningspligt fra 11.09.2026, fuld anvendelighed fra 11.12.2027.

© Embedded Systems Engineering · Schmitt Consulting S.A.R.L. · sc-sarl.com