SE

EMBEDDED SYSTEMS ENGINEERING

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

CRA-snabbkoll för enhetstillverkare

Den nya EU-lagen om cybersäkerhet för uppkopplade produkter — vad som måste vara på plats före september 2026, på ett begripligt språk.

Första bindande tidsfristen: 11 september 2026

Inte först 2027. Den som inte förbereder sig nu får ont om tid.

1 Vad det handlar om

Cyber Resilience Act — kort **CRA** — gäller sedan december 2024. Den föreskriver hur säkra uppkopplade produkter måste vara mot angrepp från internet. Den berör allt som innehåller programvara eller ansluter till ett nätverk: från den smarta termostaten till industristyrningar och appen.

Många tillverkare tror att de har tid till slutet av 2027. Det gäller bara en del av skyldigheterna. Den **första bindande tidsfristen ligger redan i september 2026** — och den gäller även produkter som sedan länge finns på marknaden och fortfarande underhålls.

11 september 2026

Rapporteringsskyldighet. Om en sårbarhet bevisligen utnyttjas av angripare måste det rapporteras till myndigheterna **inom 24 timmar**.

11 december 2027

Alla övriga skyldigheter. Produkt säker från grunden, säkerhetsuppdateringar under hela livslängden, fullständig programvaruförteckning, formell bedömning och CE-märkning.

De möjliga böterna uppgår till **15 miljoner euro eller 2,5 % av den globala årsomsättningen** — beroende på vilket belopp som är högst. Och: lagen gäller uttryckligen även för små tillverkare och enskilda leverantörer, inte bara för stora koncerner.

2 De viktigaste begreppen — kort förklarat

Firmware

Den fast inbyggda styrprogramvaran i en enhet som gör att den över huvud taget fungerar — till exempel programkoden i en maskin, en sensor eller en styrenhet.

Sårbarhet (säkerhetsbrist)

Ett fel eller en svaghet i programvaran som en angripare kan ta sig in i enheten genom eller manipulera den med.

Programvaruförteckning (SBOM)

En fullständig lista över alla programvarukomponenter i en produkt — jämförbar med stycklistan för en komponent, fast för programkoden. Utan den går det inte att säga om produkten berörs av en känd sårbarhet.

ENISA / CSIRT

ENISA är EU:s cybersäkerhetsbyrå, det centrala organet för it-säkerhet i Europa. CSIRT är de nationella statliga «datorbrandkårerna» som samordnar vid säkerhetsincidenter. Till dem går 24-timmarsrapporten.

Funktionssäkerhet

Skyddet av en enhet mot tekniska *felfunktioner och avbrott* — etablerad praxis bland annat inom fordonsteknik. CRA kompletterar detta med skydd mot *avsiktliga angrepp*.

CE-märkning

Den välkända CE-märkningen på produkter. Den bekräftar att en produkt uppfyller EU-kraven och får säljas på den europeiska marknaden.

3 Är ni CRA-redo? Checklistan

Gå igenom följande punkter. Varje ruta som ni **inte** med gott samvete kan bocka av är en öppen byggarbetsplats fram till september 2026.

ÖVERSIKT & ORGANISATION

- [ ] Vi vet vilka av våra produkter som omfattas av lagen.
- [ ] Vi vet vilka äldre produkter vi fortfarande underhåller (och som därmed också berörs).
- [ ] Det finns en ansvarig person för ämnet CRA inom företaget.

PROGRAMVARUFÖRTECKNING

- [ ] För varje produkt finns en fullständig lista över alla inbyggda programvarukomponenter.
- [ ] Vi känner i den även igen föråldrade komponenter som leverantören inte längre underhåller.
- [ ] Denna lista hålls löpande aktuell, inte upprättad en enda gång.

RAPPORTERINGSPROCESS (OBLIGATORISK FRÅN 09/2026)

- [ ] Det är reglerat vem som upptäcker en utnyttjad sårbarhet.
- [ ] Det är reglerat vem som bedömer den och vem som rapporterar den.
- [ ] Vi kan organisatoriskt faktiskt hålla 24-timmarsfristen — även på helgen.

TEKNISKT SKYDD AV ENHETEN

- [ ] Programvaran i enheten lagras krypterad och kan inte enkelt läsas ut.
- [ ] Uppdateringar är manipuleringssäkra — ingen kan smuggla in och installera programvara.
- [ ] Enheten kan ta emot säkerhetsuppdateringar under hela sin livslängd.
- [ ] Vid start kontrollerar enheten att endast äkta, oförändrad programvara körs.

BEVIS & DOKUMENTATION

- [ ] Vi kan styrka att utvecklingen följt erkända programmeringsstandarder.
- [ ] Driftsäkerhet och angreppssäkerhet tänks i ett gemensamt koncept, inte åtskilt.
- [ ] De dokument som behövs för den senare bedömningen av överensstämmelse förs med från början.

4 Hur ni går vidare

De kommande månaderna avgör om det i september 2026 finns ett ordnat förlopp eller om det måste improviseras i hast. Den som börjar tidigt fördelar arbetet — och undviker dyra nödlösningar precis före fristen. Den största hävstången ligger oftast inte i tekniken ensam, utan i det rena samspelet mellan förteckning, rapporteringsprocess och enhetsskydd.

→ Fördjupa dig & stöd

Vill ni inte bara överblicka kraven utan också genomföra dem? Tre vägar:

Facklitteratur & programvara

Praktisk kunskap från över 35 års embedded-utveckling — den tekniska grunden bakom CRA-kraven. Finns på **sc-sarl.com/sv/produkte.html**

Gratis på köpet: «Formelsamling för datavetare och ingenjörer»

Interaktiv HTML-formelsamling, 56 kapitel, tvåspråkig DE/EN, användbar offline — gratis i nedladdningsområdet.

Personligt stöd

Från programvaruförteckningen till härdning av firmware. Rådgivningssamtal på **sc-sarl.com/sv/kontakt.html**

Till produkter & nedladdningar →