SE

EMBEDDED SYSTEMS ENGINEERING

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

Verificare rapidă CRA pentru producătorii de dispozitive

Noua lege a UE privind securitatea cibernetică a produselor conectate — ce trebuie să fie pregătit până în septembrie 2026, într-un limbaj clar.

Primul termen obligatoriu: 11 septembrie 2026

Nu în 2027. Cine nu se pregătește acum va rămâne fără timp.

1 Despre ce este vorba

Cyber Resilience Act — pe scurt **CRA** — este în vigoare din decembrie 2024. Stabilește cât de sigure trebuie să fie produsele conectate împotriva atacurilor din internet. Sunt vizate toate produsele care conțin software sau se conectează la o rețea: de la termostatul inteligent la automatele industriale și la aplicație.

Mulți producători cred că au timp până la sfârșitul lui 2027. Acest lucru este valabil doar pentru o parte din obligații. **Primul termen obligatoriu este deja în septembrie 2026** — și vizează și produsele aflate de mult pe piață și încă întreținute.

11 septembrie 2026

Obligația de notificare. Dacă o vulnerabilitate este exploatată în mod dovedit de atacatori, aceasta trebuie raportată autorităților **în termen de 24 de ore**.

11 decembrie 2027

Toate celelalte obligații. Produs sigur prin proiectare, actualizări de securitate pe întreaga durată de viață, listă completă a componentelor software, evaluare formală și marcaj CE.

Amenzile posibile ajung până la **15 milioane de euro sau 2,5 % din cifra de afaceri anuală mondială** — în funcție de care sumă este mai mare. Și: legea se aplică expres și producătorilor mici și furnizorilor individuali, nu doar marilor corporații.

2 Termenii cei mai importanți — pe scurt

Firmware
Software-ul de control integrat permanent într-un dispozitiv, care face ca acesta să funcționeze — de exemplu codul de program dintr-o mașină, un senzor sau un automat.

Vulnerabilitate (breșă de securitate)
O eroare sau o slăbiciune a software-ului prin care un atacator poate pătrunde în dispozitiv sau îl poate manipula.

Listă a componentelor software (SBOM)
O listă completă a tuturor componentelor software ale unui produs — comparabilă cu lista de piese a unui component, dar pentru codul de program. Fără ea nu se poate spune dacă produsul este afectat de o breșă cunoscută.

ENISA / CSIRT
ENISA este agenția UE pentru securitate cibernetică, organismul central pentru securitatea informatică în Europa. CSIRT-urile sunt «pompierii informatici» naționali care coordonează în caz de incidente. Lor li se adresează notificarea în 24 de ore.

Siguranță funcțională
Protejarea unui dispozitiv împotriva *disfuncționalităților și defecțiunilor* tehnice — practică consacrată, de exemplu, în industria auto. CRA adaugă protecția împotriva *atacurilor intenționate*.

Marcaj CE
Binecunoscutul marcaj CE de pe produse. Confirmă că un produs respectă cerințele UE și poate fi vândut pe piața europeană.

3 Sunteți pregătit pentru CRA? Lista de verificare

Parcurgeți punctele de mai jos. Fiecare căsuță pe care **nu** o puteți bifa cu conștiința împăcată este o problemă deschisă până în septembrie 2026.

PRIVIRE DE ANSAMBLU ȘI ORGANIZARE

- [ ] Știm care dintre produsele noastre intră sub incidența legii.
- [ ] Știm ce produse mai vechi încă întreținem (și care sunt, prin urmare, de asemenea vizate).
- [ ] Există o persoană responsabilă de tema CRA în companie.

LISTA COMPONENTELOR SOFTWARE

- [ ] Pentru fiecare produs există o listă completă a tuturor componentelor software integrate.
- [ ] Recunoaștem în ea și componentele învechite pe care furnizorul nu le mai întreține.
- [ ] Această listă este menținută permanent la zi, nu creată o singură dată.

PROCES DE NOTIFICARE (OBLIGATORIU DIN 09/2026)

- [ ] Este stabilit cine observă o vulnerabilitate exploatată.
- [ ] Este stabilit cine o evaluează și cine o notifică.
- [ ] Putem respecta efectiv termenul de 24 de ore din punct de vedere organizatoric — inclusiv la sfârșit de săptămână.

PROTECȚIA TEHNICĂ A DISPOZITIVULUI

- [ ] Software-ul din dispozitiv este stocat criptat și nu poate fi citit pur și simplu.
- [ ] Actualizările sunt protejate împotriva falsificării — nimeni nu poate injecta software introdus fraudulos.
- [ ] Dispozitivul poate primi actualizări de securitate pe întreaga sa durată de viață.
- [ ] La pornire, dispozitivul verifică dacă rulează doar software autentic și nemodificat.

DOVEZI ȘI DOCUMENTAȚIE

- [ ] Putem demonstra că dezvoltarea a respectat standarde de programare recunoscute.
- [ ] Fiabilitatea și rezistența la atacuri sunt gândite într-un concept comun, nu separat.
- [ ] Documentele necesare evaluării ulterioare a conformității sunt păstrate de la bun început.

4 Cum se continuă

Lunile următoare vor decide dacă în septembrie 2026 va exista un proces ordonat sau va trebui improvizat în grabă. Cine începe devreme distribuie munca — și evită corecturi costisitoare chiar înainte de termen. Cea mai mare pârghie nu stă, de regulă, doar în tehnică, ci în buna conlucrare dintre lista componentelor, procesul de notificare și protecția dispozitivului.

→ Aprofundare și sprijin

Nu vreți doar să cuprindeți cu privirea cerințele, ci să le puneți în practică? Trei căi:

Cărți tehnice și software

Cunoștințe practice din peste 35 de ani de dezvoltare embedded — baza tehnică din spatele cerințelor CRA. Disponibile pe **sc-sarl.com/ro/produkte.html**

Cadou: «Culegere de formule pentru informaticieni și ingineri»

Culegere de formule HTML interactivă, 56 de capitole, bilingvă DE/EN, utilizabilă offline — gratuit în zona de descărcări.

Sprijin personalizat

De la lista componentelor software până la întărirea firmware-ului. Discuție de consultanță pe **sc-sarl.com/ro/kontakt.html**

Către produse și descărcări →