



EMBEDDED SYSTEMS ENGINEERING

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

Hitri pregled CRA za proizvajalce naprav

Novi zakon EU o kibernetiski varnosti povezanih izdelkov — kaj mora biti urejeno do septembra 2026, v razumljivem jeziku.

Prvi zavezujoči rok: 11. september 2026

Ne šele 2027. Kdor se zdaj ne pripravi, bo v časovni stiski.

1 Za kaj gre

Cyber Resilience Act — na kratko **CRA** — velja od decembra 2024. Predpisuje, kako varni morajo biti povezani izdelki pred napadi iz interneta. Zadeva vse, kar vsebuje programsko opremo ali se povezuje v omrežje: od pametnega termostata prek industrijskih krmilnikov do aplikacije.

Mnogi proizvajalci menijo, da imajo čas do konca leta 2027. To velja le za del obveznosti. **Prvi zavezujoči rok je že septembra 2026** — in zadeva tudi izdelke, ki so že dolgo na trgu in se še vzdržujejo.

11. september 2026

Obveznost poročanja. Če napadalci dokazljivo izkoristijo ranljivost, je treba to **v 24 urah** prijaviti organom.

11. december 2027

Vse preostale obveznosti. Izdelek varen že v zasnovi, varnostne posodobitve skozi celotno življenjsko dobo, popoln seznam programskih sestavin, formalno ocenjevanje in oznaka CE.

Možne kazni segajo do **15 milijonov evrov ali 2,5 % svetovnega letnega prometa** — kar je višje. In: zakon izrecno velja tudi za male proizvajalce in posamezne ponudnike, ne le za velike koncernne.

2 Najpomembnejši pojmi — na kratko

Strojna programska oprema (firmware)

Krmilna programska oprema, trajno vgrajena v napravo, ki poskrbi, da ta sploh deluje — na primer programska koda v stroju, senzorju ali krmilniku.

Ranljivost (varnostna luknja)

Napaka ali šibkost v programski opremi, prek katere lahko napadalec vdre v napravo ali jo manipulira.

Seznam programskih sestavin (SBOM)

Popoln seznam vseh programskih sestavin izdelka — primerljiv s kosovnico sestavnega dela, le da za programsko kodo. Brez njega ni mogoče reči, ali izdelek prizadene znana ranljivost.

ENISA / CSIRT

ENISA je agencija EU za kibernetisko varnost, osrednji organ za informacijsko varnost v Evropi. CSIRT so nacionalne državne «računalniške gasilske enote», ki usklajujejo ob varnostnih incidentih. Njim je namenjena prijava v 24 urah.

Funkcijska varnost

Zaščita naprave pred tehničnimi *okvarami in izpadi* — uveljavljena praksa na primer v avtomobilski tehniki. CRA jo dopolnjuje z zaščito pred *namernimi napadi*.

Oznaka CE

Znana oznaka CE na izdelkih. Potrjuje, da izdelek izpolnjuje zahteve EU in se sme prodajati na evropskem trgu.

3 Ste pripravljeni na CRA? Kontrolni seznam

Preglejte naslednje točke. Vsako okence, ki ga **ne** morete z mirno vestjo odkljukati, je odprta gradbena jama do septembra 2026.

PREGLED IN ORGANIZACIJA

- ☐ Vemo, kateri od naših izdelkov spadajo pod zakon.
- ☐ Vemo, katere starejše izdelke še vzdržujemo (in so torej tudi zadevani).
- ☐ V podjetju je oseba, odgovorna za temo CRA.

SEZNAM PROGRAMSKIH SESTAVIN

- ☐ Za vsak izdelek obstaja popoln seznam vseh vgrajenih programskih sestavin.
- ☐ V njem prepoznamo tudi zastarele sestavine, ki jih dobavitelj ne vzdržuje več.
- ☐ Ta seznam se sproti posodablja, ne le enkratno izdela.

POSTOPEK POROČANJA (OBVEZEN OD 09/2026)

- ☐ Določeno je, kdo opazi izkoriščeno ranljivost.
- ☐ Določeno je, kdo jo oceni in kdo jo prijavi.
- ☐ 24-urni rok lahko organizacijsko dejansko spoštujemo — tudi ob koncih tedna.

TEHNIČNA ZAŠČITA NAPRAVE

- ☐ Programska oprema v napravi je shranjena šifrirano in je ni mogoče preprosto prebrati.
- ☐ Posodobitve so zaščitene pred ponarejanjem — nihče ne more namestiti podtaknjene programske opreme.
- ☐ Naprava lahko prejema varnostne posodobitve skozi celotno življenjsko dobo.
- ☐ Ob zagonu naprava preveri, da teče le pristna, nespremenjena programska oprema.

DOKAZILA IN DOKUMENTACIJA

- ☐ Lahko izkažemo, da je razvoj potekal po priznanih programskih standardih.
- ☐ Zanesljivost in odpornost na napade sta zasnovani v enotnem konceptu, ne ločeno.
- ☐ Dokumenti, potrebni za poznejše ugotavljanje skladnosti, se vodijo od vsega začetka.

4 Kako naprej

Prihodnji meseci bodo odločili, ali bo septembra 2026 urejen potek ali pa bo treba naglo improvizirati. Kdor začne zgodaj, porazdeli delo — in se izogne dragim hitrim rešitvam tik pred rokom. Največji vzvod običajno ni le v tehniki, temveč v čistem součinkovanju seznama, postopka poročanja in zaščite naprave.

→ Poglobitev in podpora

Ne želite zahtev le pregledati, ampak jih tudi uresničiti? Tri poti:

Strokovne knjige in programska oprema

Praktično znanje iz več kot 35 let vgrajenega razvoja — tehnična podlaga za zahtevami CRA. Na voljo na sc-sarl.com/sl/produkte.html

Brezplačno zraven: «Zbirka formul za informatike in inženirje»

Interaktivna zbirka formul v HTML, 56 poglavij, dvojezična DE/EN, uporabna brez povezave — brezplačno v razdelku za prenose.

Osebna podpora

Od seznama programskih sestavin do utrjevanja strojne programske opreme. Svetovalni pogovor na sc-sarl.com/sl/kontakt.html

[Na izdelke in prenose →](#)

Ta vodnik daje praktičen pregled in ne nadomešča pravnega svetovanja. Merodajna je Uredba (EU) 2024/2847. Stanje rokov: obveznost poročanja od 11.09.2026, polna uporaba od 11.12.2027.

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