SE

EMBEDDED SYSTEMS ENGINEERING

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

Rýchly test CRA pre výrobcov zariadení

Nový zákon EÚ o kybernetickej bezpečnosti pripojených produktov — čo musí byť hotové do septembra 2026, zrozumiteľným jazykom.

Prvý záväzný termín: 11. septembra 2026

Nie až v roku 2027. Kto sa nepripraví teraz, dostane sa do časovej tiesne.

1 O čo ide

Cyber Resilience Act — skrátene **CRA** — platí od decembra 2024. Predpisuje, aké bezpečné musia byť pripojené produkty proti útokom z internetu. Týka sa všetkého, čo obsahuje softvér alebo sa pripája k sieti: od inteligentného termostatu cez priemyselné riadiace systémy až po aplikáciu.

Mnohí výrobcovia sa domnievajú, že majú čas do konca roka 2027. To platí len pre časť povinností. **Prvý záväzný termín je už v septembri 2026** — a týka sa aj produktov, ktoré sú dávno na trhu a stále sa udržiavajú.

11. septembra 2026

Ohlasovacia povinnosť. Ak je zraniteľnosť preukázateľne zneužitá útočníkmi, musí sa to **do 24 hodín** nahlásiť úradom.

11. decembra 2027

Všetky ostatné povinnosti. Produkt bezpečný od základu, bezpečnostné aktualizácie počas celej životnosti, úplný zoznam softvérových komponentov, formálne posúdenie a označenie CE.

Možné pokuty dosahujú až **15 miliónov eur alebo 2,5 % celosvetového ročného obratu** — podľa toho, ktorá suma je vyššia. A: zákon sa výslovne vzťahuje aj na malých výrobcov a jednotlivých dodávateľov, nielen na veľké koncerny.

2 Najdôležitejšie pojmy — stručne

Firmvér
Riadiaci softvér pevne zabudovaný do zariadenia, ktorý zabezpečuje, že vôbec funguje — napríklad programový kód v stroji, senzore alebo riadiacej jednotke.

Zraniteľnosť (bezpečnostná medzera)
Chyba alebo slabina v softvéri, cez ktorú môže útočník preniknúť do zariadenia alebo s ním manipulovať.

Zoznam softvérových komponentov (SBOM)
Úplný zoznam všetkých softvérových komponentov produktu — porovnateľný s kusovníkom súčiastky, ale pre programový kód. Bez neho sa nedá povedať, či je produkt zasiahnutý známou zraniteľnosťou.

ENISA / CSIRT
ENISA je agentúra EÚ pre kybernetickú bezpečnosť, ústredný orgán pre IT bezpečnosť v Európe. CSIRT sú národní štátni «počítačoví hasiči», ktorí koordinujú pri bezpečnostných incidentoch. Im je určené hlásenie do 24 hodín.

Funkčná bezpečnosť
Zabezpečenie zariadenia proti technickým *poruchám a výpadkom* — zavedená prax napríklad v automobilovej technike. CRA ju dopĺňa o ochranu proti *úmyselným útokom*.

Označenie CE
Známe označenie CE na produktoch. Potvrdzuje, že produkt spĺňa požiadavky EÚ a smie sa predávať na európskom trhu.

3 Ste pripravení na CRA? Kontrolný zoznam

Prejdite si nasledujúce body. Každé políčko, ktoré **nemôžete** s čistým svedomím zaškrtnúť, je otvorená záležitosť do septembra 2026.

PREHĽAD A ORGANIZÁCIA

- [ ] Vieme, ktoré z našich produktov spadajú pod zákon.
- [ ] Vieme, ktoré staršie produkty stále udržiavame (a sú teda takisto dotknuté).
- [ ] Vo firme je osoba zodpovedná za tému CRA.

ZOZNAM SOFTVÉROVÝCH KOMPONENTOV

- [ ] Pre každý produkt existuje úplný zoznam všetkých zabudovaných softvérových komponentov.
- [ ] Rozpoznávame v ňom aj zastarané komponenty, ktoré dodávateľ už neudržiava.
- [ ] Tento zoznam sa priebežne udržiava aktuálny, nie je vytvorený jednorazovo.

OHLASOVACÍ PROCES (POVINNÝ OD 09/2026)

- [ ] Je stanovené, kto zaznamená zneužitú zraniteľnosť.
- [ ] Je stanovené, kto ju posúdi a kto ju nahlási.
- [ ] Dokážeme organizačne skutočne dodržať 24-hodinovú lehotu — aj cez víkend.

TECHNICKÉ ZABEZPEČENIE ZARIADENIA

- [ ] Softvér v zariadení je uložený šifrovane a nedá sa len tak prečítať.
- [ ] Aktualizácie sú odolné proti falšovaniu — nikto nemôže nasadiť podstrčený softvér.
- [ ] Zariadenie môže prijímať bezpečnostné aktualizácie počas celej životnosti.
- [ ] Pri štarte zariadenie kontroluje, že beží iba pravý, nezmenený softvér.

DÔKAZY A DOKUMENTÁCIA

- [ ] Dokážeme doložiť, že vývoj prebiehal podľa uznávaných programovacích štandardov.
- [ ] Spoľahlivosť a odolnosť proti útokom sú poňaté v jednom spoločnom koncepte, nie oddelene.
- [ ] Dokumenty potrebné pre neskoršie posúdenie zhody sa vedú od začiatku.

4 Ako ďalej

Nasledujúce mesiace rozhodnú, či v septembri 2026 bude riadny priebeh, alebo sa bude musieť zbrklo improvizovať. Kto začne včas, rozloží prácu — a vyhne sa drahým rýchlym riešeniam tesne pred termínom. Najväčšia páka zvyčajne neleží len v technike, ale v čistej súhre zoznamu, ohlasovacieho procesu a zabezpečenia zariadenia.

→ Hlbšie & podpora

Nechcete požiadavky len prehliadnuť, ale uviesť ich do praxe? Tri cesty:

Odborné knihy a softvér

Praktické znalosti z viac ako 35 rokov vývoja vstavaných systémov — technický základ za požiadavkami CRA. Nájdete na **sc-sarl.com/sk/produkte.html**

Zdarma k tomu: «Zbierka vzorcov pre informatikov a inžinierov»

Interaktívna HTML zbierka vzorcov, 56 kapitol, dvojjazyčná DE/EN, použiteľná offline — zdarma v sekcii sťahovania.

Osobná podpora

Od zoznamu softvérových komponentov po posilnenie firmvéru. Konzultácia na **sc-sarl.com/sk/kontakt.html**

K produktom a na stiahnutie →

Tento sprievodca poskytuje praktický prehľad a nenahrádza právne poradenstvo. Rozhodujúce je nariadenie (EÚ) 2024/2847. Stav lehôt: ohlasovacia povinnosť od 11.09.2026, plná uplatniteľnosť od 11.12.2027.