



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

Rychlý test CRA pro výrobce zařízení

Nový zákon EU o kybernetické bezpečnosti připojených produktů — co musí být hotové do září 2026, srozumitelným jazykem.

První závazný termín: 11. září 2026

Ne až v roce 2027. Kdo se nepřipraví teď, dostane se do časové tísně.

1 O co jde

Cyber Resilience Act — zkráceně **CRA** — je v platnosti od prosince 2024. Předepisuje, jak bezpečné musí být připojené produkty proti útokům z internetu. Týká se všeho, co obsahuje software nebo se připojuje k síti: od chytrého termostatu přes průmyslové řídicí systémy až po aplikaci.

Mnozí výrobci se domnívají, že mají čas do konce roku 2027. To platí jen pro část povinností. **První závazný termín je už v září 2026** — a týká se i produktů, které jsou dávno na trhu a stále se udržují.

11. září 2026

Ohlašovací povinnost. Je-li zranitelnost prokazatelně zneužita útočníky, musí se to **do 24 hodin** nahlásit úřadům.

11. prosince 2027

Všechny ostatní povinnosti. Produkt bezpečný od základu, bezpečnostní aktualizace po celou dobu životnosti, úplný soupis softwarových součástí, formální posouzení a označení CE.

Možné pokuty dosahují až **15 milionů eur nebo 2,5 % celosvětového ročního obrátu** — podle toho, která částka je vyšší. A: zákon se výslovně vztahuje i na malé výrobce a jednotlivé dodavatele, nejen na velké koncerny.

2 Nejdůležitější pojmy — stručně

Firmware

Řídicí software pevně zabudovaný do zařízení, který zajišťuje, že vůbec funguje — například programový kód ve stroji, senzoru nebo řídicí jednotce.

Zranitelnost (bezpečnostní mezera)

Chyba nebo slabina v softwaru, jejímž prostřednictvím může útočník proniknout do zařízení nebo s ním manipulovat.

Soupis softwarových součástí (SBOM)

Úplný seznam všech softwarových součástí produktu — srovnatelný s kusovníkem součástky, ale pro programový kód. Bez něj nelze říci, zda je produkt zasažen známou zranitelností.

ENISA / CSIRT

ENISA je agentura EU pro kybernetickou bezpečnost, ústřední orgán pro IT bezpečnost v Evropě. CSIRT jsou národní státní «počítačová hasiči», kteří koordinují při bezpečnostních incidentech. Jim je určeno hlášení do 24 hodin.

Funkční bezpečnost

Zabezpečení zařízení proti technickým *poruchám a výpadkům* — zavedená praxe například v automobilové technice. CRA ji doplňuje o ochranu proti *úmyslným útokům*.

Označení CE

Známé označení CE na produktech. Potvrzuje, že produkt splňuje požadavky EU a smí být prodáván na evropském trhu.

3 Jste připraveni na CRA? Kontrolní seznam

Projděte následující body. Každé okénko, které **nemůžete** s čistým svědomím zaškrtnout, je otevřená záležitost do září 2026.

PŘEHLED A ORGANIZACE

- ☐ Víme, které z našich produktů spadají pod zákon.
- ☐ Víme, které starší produkty stále udržujeme (a jsou tedy rovněž dotčeny).
- ☐ Ve firmě je osoba odpovědná za téma CRA.

SOUVIS SOFTWAROVÝCH SOUČÁSTÍ

- ☐ Pro každý produkt existuje úplný seznam všech zabudovaných softwarových součástí.
- ☐ Rozpoznáváme v něm i zastaralé komponenty, které dodavatel již neudrží.
- ☐ Tento seznam je průběžně udržován aktuální, nikoli vytvořen jednorázově.

OHLAŠOVACÍ PROCES (POVINNÝ OD 09/2026)

- ☐ Je stanoveno, kdo zaznamená zneužitou zranitelnost.
- ☐ Je stanoveno, kdo ji posoudí a kdo ji nahlásí.
- ☐ Dokážeme organizačně skutečně dodržet 24hodinovou lhůtu — i o víkendu.

TECHNICKÉ ZABEZPEČENÍ ZAŘÍZENÍ

- ☐ Software v zařízení je uložen šifrovaně a nelze ho jen tak přechytit.
- ☐ Aktualizace jsou odolné proti padělání — nikdo nemůže nasadit podstrčený software.
- ☐ Zařízení může přijímat bezpečnostní aktualizace po celou dobu životnosti.
- ☐ Při startu zařízení kontroluje, že běží pouze pravý, nezměněný software.

DŮKAZY A DOKUMENTACE

- ☐ Dokážeme doložit, že vývoj probíhal podle uznávaných programovacích standardů.
- ☐ Spolehlivost a odolnost proti útokům jsou pojaty v jednom společném konceptu, nikoli odděleně.
- ☐ Dokumenty potřebné pro pozdější posouzení shody jsou vedeny od začátku.

4 Jak dál

Nadcházející měsíce rozhodnou, zda v září 2026 bude řádný průběh, nebo se bude muset zbrkle improvizovat. Kdo začne včas, rozloží práci — a vyhne se drahým rychlým řešením těsně před termínem. Největší páka obvykle neleží jen v technice, ale v čisté souhře soupisu, ohlašovacího procesu a zabezpečení zařízení.

→ Hlouběji & podpora

Nechcete požadavky jen přehlédnout, ale uvést je do praxe? Tři cesty:

Odborné knihy a software

Praktické znalosti z více než 35 let vývoje vestavných systémů — technický základ za požadavky CRA. K nalezení na sc-sarl.com/cs/produkty.html

Zdarma k tomu: «Sbírka vzorců pro informatiky a inženýry»

Interaktivní HTML sbírka vzorců, 56 kapitol, dvojjazyčná DE/EN, použitelná offline — zdarma v sekci stahování.

Osobní podpora

Od soupisu softwarových součástí po posílení firmwaru. Konzultace na sc-sarl.com/cs/kontakt.html

K produktům a ke stažení →

Tento průvodce poskytuje praktický přehled a nenahrazuje právní poradenství. Rozhodující je nařízení (EU) 2024/2847. Stav lhůt: ohlašovací povinnost od 11.09.2026, plná použitelnost od 11.12.2027.

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