SE

EMBEDDED SYSTEMS ENGINEERING

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

Check rapido CRA per produttori di dispositivi

La nuova legge UE sulla sicurezza informatica dei prodotti connessi — ciò che deve essere pronto entro settembre 2026, in un linguaggio comprensibile.

Prima scadenza vincolante: 11 settembre 2026

Non il 2027. Chi non si prepara ora rischia di restare senza tempo.

1 Di cosa si tratta

Il **Cyber Resilience Act** — in breve **CRA** — è in vigore da dicembre 2024. Stabilisce quanto sicuri debbano essere i prodotti connessi contro gli attacchi provenienti da internet. Riguarda tutto ciò che contiene software o si collega a una rete: dal termostato smart agli automi industriali fino all'app.

Molti produttori credono di avere tempo fino alla fine del 2027. Questo vale solo per una parte degli obblighi. La **prima scadenza vincolante cade già a settembre 2026** — e riguarda anche i prodotti da tempo sul mercato e ancora mantenuti.

11 settembre 2026

Obbligo di notifica. Se una vulnerabilità viene dimostrabilmente sfruttata da aggressori, deve essere notificata alle autorità **entro 24 ore**.

11 dicembre 2027

Tutti gli altri obblighi. Prodotto sicuro fin dalla progettazione, aggiornamenti di sicurezza per tutto il ciclo di vita, distinta software completa, valutazione formale e marcatura CE.

Le possibili sanzioni arrivano fino a **15 milioni di euro o il 2,5 % del fatturato annuo mondiale** — a seconda dell'importo maggiore. E: la legge si applica espressamente anche ai piccoli produttori e ai singoli fornitori, non solo alle grandi aziende.

2 I termini più importanti — in breve

Firmware
Il software di controllo integrato in modo permanente in un dispositivo che ne consente il funzionamento — ad esempio il codice di programma in una macchina, un sensore o un'unità di controllo.

Vulnerabilità (falla di sicurezza)
Un errore o una debolezza del software attraverso cui un aggressore può penetrare nel dispositivo o manipolarlo.

Distinta software (SBOM)
Un elenco completo di tutti i componenti software di un prodotto — paragonabile alla distinta di un componente, ma per il codice di programma. Senza di essa non è possibile sapere se il prodotto è interessato da una falla nota.

ENISA / CSIRT
L'ENISA è l'agenzia UE per la cibersicurezza, l'organo centrale per la sicurezza informatica in Europa. I CSIRT sono i «vigili del fuoco informatici» nazionali che coordinano in caso di incidenti. A loro va la notifica entro 24 ore.

Sicurezza funzionale
La protezione di un dispositivo contro *malfunzionamenti e guasti* tecnici — prassi consolidata, ad esempio, nell'automotive. Il CRA vi aggiunge la protezione contro gli *attacchi intenzionali*.

Marcatura CE
La nota marcatura CE sui prodotti. Conferma che un prodotto soddisfa i requisiti UE e può essere venduto sul mercato europeo.

3 Siete pronti per il CRA? La checklist

Esaminate i punti seguenti. Ogni casella che **non** potete spuntare con coscienza tranquilla è un cantiere aperto fino a settembre 2026.

PANORAMICA E ORGANIZZAZIONE

- [ ] Sappiamo quali dei nostri prodotti rientrano nella legge.
- [ ] Sappiamo quali prodotti più vecchi manteniamo ancora (e che sono quindi anch'essi interessati).
- [ ] Esiste una persona responsabile del tema CRA in azienda.

DISTINTA SOFTWARE

- [ ] Per ogni prodotto esiste un elenco completo di tutti i componenti software integrati.
- [ ] Vi riconosciamo anche i componenti obsoleti che il fornitore non mantiene più.
- [ ] Questo elenco viene tenuto costantemente aggiornato, non creato una sola volta.

PROCESSO DI NOTIFICA (OBBLIGATORIO DA 09/2026)

- [ ] È stabilito chi rileva una vulnerabilità sfruttata.
- [ ] È stabilito chi la valuta e chi la notifica.
- [ ] Possiamo rispettare davvero il termine di 24 ore sul piano organizzativo — anche nel fine settimana.

PROTEZIONE TECNICA DEL DISPOSITIVO

- [ ] Il software nel dispositivo è memorizzato cifrato e non può essere semplicemente letto.
- [ ] Gli aggiornamenti sono a prova di manomissione — nessuno può iniettare software introdotto di nascosto.
- [ ] Il dispositivo può ricevere aggiornamenti di sicurezza per tutto il suo ciclo di vita.
- [ ] All'avvio il dispositivo verifica che venga eseguito solo software autentico e non alterato.

PROVE E DOCUMENTAZIONE

- [ ] Possiamo dimostrare che lo sviluppo ha seguito standard di programmazione riconosciuti.
- [ ] Affidabilità e resistenza agli attacchi sono pensate in un concetto comune, non separato.
- [ ] I documenti necessari per la successiva valutazione di conformità vengono tenuti fin dall'inizio.

4 Come si prosegue

I prossimi mesi decideranno se a settembre 2026 ci sarà un processo ordinato o se si dovrà improvvisare in fretta. Chi inizia presto distribuisce il lavoro — ed evita costose correzioni dell'ultimo minuto poco prima della scadenza. La leva maggiore non sta di solito nella sola tecnica, ma nella corretta interazione tra distinta software, processo di notifica e protezione del dispositivo.

→ Approfondire e supporto

Non volete solo avere una panoramica dei requisiti, ma attuarli? Tre strade:

> **Libri tecnici e software**
> Conoscenze pratiche maturate in oltre 35 anni di sviluppo embedded — la base tecnica dietro i requisiti del CRA. Disponibili su **sc-sarl.com/it/produkte.html**

> **In omaggio: «Raccolta di formule per informatici e ingegneri»**
> Raccolta di formule HTML interattiva, 56 capitoli, bilingue DE/EN, utilizzabile offline — gratis nell'area download.

> **Supporto personalizzato**
> Dalla distinta software all'hardening del firmware. Colloquio di consulenza su **sc-sarl.com/it/kontakt.html**

Ai prodotti e download →

Questa guida offre una panoramica pratica e non sostituisce una consulenza legale. Il testo di riferimento è il regolamento (UE) 2024/2847. Stato delle scadenze: obbligo di notifica dall'11/09/2026, piena applicabilità dall'11/12/2027.