SE

EMBEDDED SYSTEMS ENGINEERING

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

CRA-pikatarkistus laitevalmistajille

Uusi EU:n laki verkkoon liitettyjen tuotteiden kyberturvallisuudesta — mitä on oltava kunnossa syyskuuhun 2026 mennessä, ymmärrettävällä kielellä.

Ensimmäinen sitova määräaika: 11. syyskuuta 2026

Ei vasta 2027. Joka ei valmistaudu nyt, joutuu aikapulaan.

1 Mistä on kyse

Cyber Resilience Act — lyhyesti **CRA** — on ollut voimassa joulukuusta 2024. Se määrää, kuinka turvallisia verkkoon liitettyjen tuotteiden on oltava internetistä tulevia hyökkäyksiä vastaan. Se koskee kaikkea, mikä sisältää ohjelmistoa tai liittyy verkkoon: älytermostaatista teollisuusohjaimiin ja sovellukseen.

Monet valmistajat luulevat, että aikaa on vuoden 2027 loppuun. Se pätee vain osaan velvoitteista. **Ensimmäinen sitova määräaika on jo syyskuussa 2026** — ja se koskee myös tuotteita, jotka ovat jo kauan olleet markkinoilla ja joita yhä ylläpidetään.

11. syyskuuta 2026

Ilmoitusvelvollisuus. Jos hyökkääjät todistettavasti käyttävät haavoittuvuutta hyväkseen, siitä on ilmoitettava viranomaisille **24 tunnin kuluessa**.

11. joulukuuta 2027

Kaikki muut velvoitteet. Tuote turvallinen perusteista lähtien, tietoturvapäivitykset koko elinkaaren ajan, täydellinen ohjelmiston osaluettelo, virallinen arviointi ja CE-merkintä.

Mahdolliset sakot yltävät **15 miljoonaan euroon tai 2,5 prosenttiin maailmanlaajuisesta vuosiliikevaihdosta** — sen mukaan, kumpi on suurempi. Ja: laki koskee nimenomaisesti myös pieniä valmistajia ja yksittäisiä toimittajia, ei vain suuryrityksiä.

2 Tärkeimmät käsitteet — lyhyesti

Laiteohjelmisto (firmware)
Laitteeseen kiinteästi sisäänrakennettu ohjausohjelmisto, joka saa sen ylipäätään toimimaan — esimerkiksi koneen, anturin tai ohjaimen ohjelmakoodi.

Haavoittuvuus (turva-aukko)
Ohjelmiston virhe tai heikkous, jonka kautta hyökkääjä voi tunkeutua laitteeseen tai manipuloida sitä.

Ohjelmiston osaluettelo (SBOM)
Täydellinen luettelo kaikista tuotteen ohjelmisto-osista — verrattavissa komponentin osaluetteloon, mutta ohjelmakoodille. Ilman sitä ei voida sanoa, koskeeko tunnettu haavoittuvuus tuotetta.

ENISA / CSIRT
ENISA on EU:n kyberturvallisuusvirasto, Euroopan tietoturvan keskuselin. CSIRT-ryhmät ovat kansallisia valtiollisia «tietokonepalokuntia», jotka koordinoivat tietoturvapoikkeamissa. Niille menee 24 tunnin ilmoitus.

Toiminnallinen turvallisuus
Laitteen suojaaminen teknisiltä *toimintahäiriöiltä ja vioilta* — vakiintunut käytäntö esimerkiksi ajoneuvotekniikassa. CRA täydentää tätä suojalla *tahallisia hyökkäyksiä* vastaan.

CE-merkintä
Tunnettu CE-merkki tuotteissa. Se vahvistaa, että tuote täyttää EU:n vaatimukset ja sitä saa myydä Euroopan markkinoilla.

3 Oletteko CRA-valmiita? Tarkistuslista

Käykää läpi seuraavat kohdat. Jokainen ruutu, jota **ette** voi hyvällä omallatunnolla rastittaa, on avoin työmaa syyskuuhun 2026 saakka.

YLEISKUVA & ORGANISOINTI

- [ ] Tiedämme, mitkä tuotteistamme kuuluvat lain piiriin.
- [ ] Tiedämme, mitä vanhempia tuotteita yhä ylläpidämme (ja jotka siten kuuluvat myös lain piiriin).
- [ ] Yrityksessä on CRA-aiheesta vastaava henkilö.

OHJELMISTON OSALUETTELO

- [ ] Jokaisesta tuotteesta on täydellinen luettelo kaikista sisäänrakennetuista ohjelmisto-osista.
- [ ] Tunnistamme siitä myös vanhentuneet osat, joita toimittaja ei enää ylläpidä.
- [ ] Tätä luetteloa pidetään jatkuvasti ajan tasalla, ei laadita vain kerran.

ILMOITUSPROSESSI (PAKOLLINEN 09/2026 ALKAEN)

- [ ] On määritelty, kuka havaitsee hyväksikäytetyn haavoittuvuuden.
- [ ] On määritelty, kuka arvioi sen ja kuka ilmoittaa siitä.
- [ ] Pystymme organisatorisesti todella noudattamaan 24 tunnin määräaikaa — myös viikonloppuna.

LAITTEEN TEKNINEN SUOJAUS

- [ ] Laitteen ohjelmisto on tallennettu salattuna eikä sitä voi noin vain lukea ulos.
- [ ] Päivitykset ovat väärentämissuojattuja — kukaan ei voi asentaa salakuljetettua ohjelmistoa.
- [ ] Laite voi vastaanottaa tietoturvapäivityksiä koko elinkaarensa ajan.
- [ ] Käynnistyessään laite tarkistaa, että vain aitoa, muuttamatonta ohjelmistoa ajetaan.

TODISTEET & DOKUMENTAATIO

- [ ] Voimme osoittaa, että kehitys on tehty tunnustettujen ohjelmointistandardien mukaisesti.
- [ ] Toimintavarmuus ja hyökkäysturvallisuus on ajateltu yhteisenä kokonaisuutena, ei erikseen.
- [ ] Myöhempää vaatimustenmukaisuuden arviointia varten tarvittavat asiakirjat pidetään mukana alusta alkaen.

4 Miten edetä

Tulevat kuukaudet ratkaisevat, onko syyskuussa 2026 hallittu prosessi vai joudutaanko improvisoimaan kiireellä. Joka aloittaa ajoissa, jakaa työn — ja välttää kalliit hätäratkaisut juuri ennen määräaikaa. Suurin vipuvarsi ei yleensä ole tekniikassa yksin, vaan osaluettelon, ilmoitusprosessin ja laitteen suojauksen sujuvassa yhteispelissä.

→ Syvenny & tuki

Ettekö halua vain saada yleiskuvaa vaatimuksista vaan myös toteuttaa ne? Kolme tietä:

Ammattikirjat & ohjelmistot

Käytännön tietoa yli 35 vuoden sulautetun kehityksen ajalta — CRA-vaatimusten tekninen perusta. Löytyy osoitteesta **sc-sarl.com/fi/produkte.html**

Kaupan päälle: «Kaavakokoelma tietojenkäsittelijöille ja insinööreille»

Interaktiivinen HTML-kaavakokoelma, 56 lukua, kaksikielinen DE/EN, käytettävissä offline-tilassa — ilmaiseksi latausalueella.

Henkilökohtainen tuki

Ohjelmiston osaluettelosta laiteohjelmiston koventamiseen. Neuvottelu osoitteessa **sc-sarl.com/fi/kontakt.html**

Tuotteisiin & latauksiin →

Tämä opas antaa käytännönläheisen yleiskuvan eikä korvaa oikeudellista neuvontaa. Määräävä on asetus (EU) 2024/2847. Määräaikojen tila: ilmoitusvelvollisuus 11.9.2026 alkaen, täysi sovellettavuus 11.12.2027 alkaen.